

**kaspersky**

# **Kaspersky Security для Windows Server**

Руководство администратора

*Версия программы: 11*

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 02.10.2020

© АО «Лаборатория Касперского», 2020. Все права защищены.

<https://www.kaspersky.ru>  
<https://support.kaspersky.ru>

О "Лаборатории Касперского" (<https://www.kaspersky.ru/about/company>)

# Содержание

|                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------|----|
| Об этом документе .....                                                                                 | 17 |
| Источники информации о Kaspersky Security для Windows Server .....                                      | 18 |
| Источники для самостоятельного поиска информации .....                                                  | 18 |
| Обсуждение программ "Лаборатории Касперского" в сообществе пользователей .....                          | 19 |
| О программе .....                                                                                       | 20 |
| Требования .....                                                                                        | 21 |
| Аппаратные и программные требования .....                                                               | 21 |
| Требования к серверу, на который устанавливается Kaspersky Security для Windows Server .....            | 21 |
| Требования к защищаемому сетевому хранилищу .....                                                       | 23 |
| Требования к устройству, на котором устанавливается Консоль программы .....                             | 24 |
| Указания по эксплуатации и требования к среде .....                                                     | 26 |
| Kaspersky Endpoint Agent .....                                                                          | 27 |
| Подготовка к установке программы .....                                                                  | 28 |
| Установка и удаление программы .....                                                                    | 29 |
| Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows ..... | 29 |
| Программные компоненты Kaspersky Security для Windows Server .....                                      | 30 |
| Программные компоненты набора Средства администрирования .....                                          | 34 |
| Изменения в системе после установки Kaspersky Security для Windows Server .....                         | 34 |
| Процессы Kaspersky Security для Windows Server .....                                                    | 38 |
| Параметры установки и удаления и ключи командной строки для службы установщика Windows .....            | 38 |
| Журналы установки и удаления Kaspersky Security для Windows Server .....                                | 42 |
| Планирование установки .....                                                                            | 42 |
| Выбор средств администрирования .....                                                                   | 43 |
| Выбор способа установки .....                                                                           | 44 |
| Установка и удаление программы с помощью мастера .....                                                  | 45 |
| Установка с помощью мастера установки .....                                                             | 45 |
| Изменение состава компонентов и восстановление Kaspersky Security для Windows Server .....              | 57 |
| Удаление с помощью мастера установки .....                                                              | 58 |
| Установка и удаление программы из командной строки .....                                                | 61 |
| Об установке и удалении Kaspersky Security для Windows Server из командной строки .....                 | 61 |
| Примеры команд установки Kaspersky Security для Windows Server .....                                    | 62 |
| Действия после установки Kaspersky Security для Windows Server .....                                    | 64 |
| Добавление и удаление компонентов. Примеры команд .....                                                 | 65 |
| Удаление Kaspersky Security для Windows Server. Примеры команд .....                                    | 66 |
| Коды возврата .....                                                                                     | 67 |

|                                                                                                                       |     |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| Установка и удаление программы с помощью Kaspersky Security Center .....                                              | 68  |
| Общие сведения об установке через Kaspersky Security Center .....                                                     | 68  |
| Права для установки или удаления Kaspersky Security для Windows Server .....                                          | 68  |
| Установка Kaspersky Security для Windows Server через Kaspersky Security Center .....                                 | 69  |
| Действия после установки Kaspersky Security для Windows Server .....                                                  | 71  |
| Установка Консоли программы через Kaspersky Security Center .....                                                     | 72  |
| Удаление Kaspersky Security для Windows Server через Kaspersky Security Center .....                                  | 73  |
| Установка и удаление программы через групповые политики Active Directory .....                                        | 73  |
| Установка Kaspersky Security для Windows Server через групповые политики Active Directory .....                       | 73  |
| Действия после установки Kaspersky Security для Windows Server .....                                                  | 74  |
| Удаление Kaspersky Security для Windows Server через групповые политики Active Directory .....                        | 75  |
| Проверка функций Kaspersky Security для Windows Server. Использование тестового вируса EICAR ..                       | 76  |
| О тестовом вирусе EICAR .....                                                                                         | 76  |
| Проверка функций постоянной защиты файлов и проверки по требованию .....                                              | 77  |
| Процедура приемки .....                                                                                               | 79  |
| Безопасное состояние .....                                                                                            | 79  |
| Проверка работоспособности. EICAR .....                                                                               | 86  |
| Проверка целостности компонентов программы .....                                                                      | 90  |
| Разделение доступа к функциям программы по пользовательским ролям .....                                               | 92  |
| О правах на управление Kaspersky Security для Windows Server .....                                                    | 92  |
| О правах на управление службой Kaspersky Security Service .....                                                       | 94  |
| О правах доступа к службе Kaspersky Security Management .....                                                         | 96  |
| Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service ..... | 96  |
| Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля .....                                | 98  |
| Разрешение сетевых соединений для службы Kaspersky Security Management Service .....                                  | 101 |
| Интерфейс программы .....                                                                                             | 102 |
| Работа с Плагином управления .....                                                                                    | 103 |
| Управление Kaspersky Security для Windows Server из Kaspersky Security Center .....                                   | 103 |
| Управление параметрами программы .....                                                                                | 104 |
| Навигация .....                                                                                                       | 104 |
| Настройка общих параметров программы в Kaspersky Security Center .....                                                | 105 |
| Настройка параметров карантина и резервного хранилища в Kaspersky Security Center .....                               | 112 |
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы .....                                                     | 113 |
| Создание и настройка политик .....                                                                                    | 116 |
| Создание политики .....                                                                                               | 117 |
| Разделы параметров политики Kaspersky Security для Windows Server .....                                               | 119 |
| Настройка политики .....                                                                                              | 124 |
| Создание и настройка задач в Kaspersky Security Center .....                                                          | 126 |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| О создании задач в Kaspersky Security Center .....                                                                 | 126 |
| Создание задачи в Kaspersky Security Center .....                                                                  | 127 |
| Настройка локальных задач в окне Параметры программы в Kaspersky Security Center .....                             | 129 |
| Настройка групповых задач в Kaspersky Security Center .....                                                        | 130 |
| Настройка параметров диагностики сбоев в Kaspersky Security Center .....                                           | 139 |
| Работа с расписанием задач .....                                                                                   | 141 |
| Отчеты в Kaspersky Security Center .....                                                                           | 144 |
| Работа с Консолью Kaspersky Security для Windows Server .....                                                      | 147 |
| О Консоли Kaspersky Security для Windows Server .....                                                              | 147 |
| Интерфейс Консоли Kaspersky Security для Windows Server .....                                                      | 148 |
| Окно Консоли Kaspersky Security для Windows Server .....                                                           | 148 |
| Значок области уведомлений в панели задач .....                                                                    | 152 |
| Управление Kaspersky Security для Windows Server через Консоль программы, установленную на другом устройстве ..... | 153 |
| Настройка общих параметров программы в Консоли программы .....                                                     | 153 |
| Управление задачами Kaspersky Security для Windows Server .....                                                    | 160 |
| Категории задач Kaspersky Security для Windows Server .....                                                        | 160 |
| Запуск / приостановка / возобновление / остановка задачи вручную .....                                             | 161 |
| Работа с расписанием задач .....                                                                                   | 162 |
| Использование учетных записей для запуска задач .....                                                              | 164 |
| Импорт и экспорт параметров .....                                                                                  | 165 |
| Использование шаблонов параметров безопасности .....                                                               | 169 |
| Просмотр состояния защиты и информации о Kaspersky Security для Windows Server .....                               | 172 |
| Работа с Веб-плагином .....                                                                                        | 178 |
| Управление Kaspersky Security для Windows Server из Kaspersky Security Center Web Console .....                    | 178 |
| Ограничения Веб-плагина .....                                                                                      | 179 |
| Управление параметрами программы .....                                                                             | 179 |
| Настройка общих параметров программы в Kaspersky Security Center Web Console .....                                 | 180 |
| Настройка параметров карантина и резервного хранилища с помощью Веб-плагина .....                                  | 185 |
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы .....                                                  | 186 |
| Создание и настройка политик .....                                                                                 | 189 |
| Создание политики .....                                                                                            | 190 |
| Разделы параметров политики Kaspersky Security для Windows Server .....                                            | 191 |
| Создание и настройка задач в Kaspersky Security Center .....                                                       | 196 |
| О создании задач в Kaspersky Security Center Web Console .....                                                     | 196 |
| Создание задачи в Kaspersky Security Center Web Console .....                                                      | 197 |
| Настройка групповых задач в Kaspersky Security Center .....                                                        | 198 |
| Настройка параметров диагностики сбоев в Kaspersky Security Center .....                                           | 199 |
| Работа с расписанием задач .....                                                                                   | 202 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Отчеты в Kaspersky Security Center.....                                                          | 204 |
| Диагностическое окно .....                                                                       | 206 |
| О диагностическом окне.....                                                                      | 206 |
| Просмотр состояния Kaspersky Security для Windows Server с помощью диагностического окна .....   | 207 |
| Просмотр статистики событий безопасности.....                                                    | 208 |
| Просмотр текущей активности программы.....                                                       | 208 |
| Настройка записи файлов дампов и файлов трассировки .....                                        | 209 |
| Обновление баз и модулей Kaspersky Security для Windows Server .....                             | 211 |
| О задачах обновления .....                                                                       | 211 |
| Об обновлении модулей программы .....                                                            | 212 |
| Об обновлении баз программы .....                                                                | 213 |
| Схемы обновления баз и модулей антивирусных программ в организации.....                          | 214 |
| Настройка задач обновления .....                                                                 | 217 |
| Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server ..... | 217 |
| Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы .....             | 220 |
| Настройка параметров задачи Копирование обновлений .....                                         | 222 |
| Настройка параметров задачи Обновление модулей программы.....                                    | 222 |
| Откат обновления баз Kaspersky Security для Windows Server .....                                 | 224 |
| Откат обновления программных модулей.....                                                        | 224 |
| Статистика задач обновления .....                                                                | 224 |
| Изолирование и резервное копирование объектов.....                                               | 226 |
| Изолирование возможно зараженных объектов. Карантин .....                                        | 226 |
| Об изолировании возможно зараженных объектов .....                                               | 226 |
| Просмотр объектов на карантине .....                                                             | 227 |
| Проверка объектов на карантине .....                                                             | 228 |
| Восстановление содержимого карантина .....                                                       | 230 |
| Помещение объектов на карантин.....                                                              | 232 |
| Удаление объектов с карантина.....                                                               | 232 |
| Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" .....          | 233 |
| Настройка параметров карантина.....                                                              | 234 |
| Статистика карантина .....                                                                       | 235 |
| Резервное копирование объектов. Резервное хранилище.....                                         | 236 |
| О резервном копировании объектов перед лечением или удалением .....                              | 236 |
| Просмотр объектов в резервном хранилище.....                                                     | 237 |
| Восстановление файлов из резервного хранилища .....                                              | 239 |
| Удаление файлов из резервного хранилища .....                                                    | 241 |
| Настройка параметров резервного хранилища .....                                                  | 241 |
| Статистика резервного хранилища.....                                                             | 242 |

|                                                                                                                       |     |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы .....                                                     | 243 |
| О хранилище заблокированных узлов.....                                                                                | 243 |
| Включение блокировки недоверенных узлов.....                                                                          | 244 |
| Настройка параметров хранилища заблокированных узлов.....                                                             | 245 |
| Регистрация событий. Журналы Kaspersky Security для Windows Server .....                                              | 246 |
| Способы записи событий Kaspersky Security для Windows Server.....                                                     | 246 |
| Журнал системного аудита .....                                                                                        | 247 |
| Сортировка событий в журнале системного аудита.....                                                                   | 247 |
| Фильтрация событий в журнале системного аудита .....                                                                  | 248 |
| Удаление событий из журнала системного аудита .....                                                                   | 249 |
| Журналы выполнения задач.....                                                                                         | 249 |
| О журналах выполнения задач .....                                                                                     | 250 |
| Сортировка журналов выполнения задач .....                                                                            | 250 |
| Фильтрация журналов выполнения задач.....                                                                             | 250 |
| Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в<br>журналах выполнения задач ..... | 251 |
| Экспорт информации из журнала выполнения задачи .....                                                                 | 252 |
| Удаление журналов выполнения задач.....                                                                               | 252 |
| Журнал безопасности.....                                                                                              | 253 |
| Просмотр журнала событий Kaspersky Security для Windows Server в оснастке Просмотр событий ..                         | 253 |
| Настройка параметров журналов с помощью Плагина управления .....                                                      | 254 |
| Об интеграции с SIEM .....                                                                                            | 257 |
| Настройка параметров интеграции с SIEM .....                                                                          | 257 |
| Настройка журналов и уведомлений .....                                                                                | 260 |
| Настройка параметров журналов.....                                                                                    | 261 |
| Журнал безопасности .....                                                                                             | 262 |
| Настройка параметров интеграции с SIEM .....                                                                          | 262 |
| Настройка параметров уведомлений .....                                                                                | 265 |
| Настройка обмена информацией с Сервером администрирования .....                                                       | 266 |
| Настройка уведомлений.....                                                                                            | 268 |
| Способы уведомления администратора и пользователей .....                                                              | 268 |
| Настройка уведомлений администратора и пользователей .....                                                            | 269 |
| Запуск и остановка Kaspersky Security для Windows Server .....                                                        | 272 |
| Запуск Плагина управления Kaspersky Security для Windows Server .....                                                 | 272 |
| Запуск Консоли Kaspersky Security для Windows Server из меню Пуск .....                                               | 272 |
| Запуск и остановка службы Kaspersky Security.....                                                                     | 273 |
| Запуск компонентов Kaspersky Security для Windows Server при безопасном режиме загрузки<br>операционной системы ..... | 274 |
| О работе Kaspersky Security для Windows Server при безопасном режиме загрузки<br>операционной системы .....           | 274 |

|                                                                                                     |     |
|-----------------------------------------------------------------------------------------------------|-----|
| Запуск Kaspersky Security для Windows Server в безопасном режиме .....                              | 275 |
| Механизмы самозащиты Kaspersky Security для Windows Server .....                                    | 276 |
| О механизмах самозащиты Kaspersky Security для Windows Server .....                                 | 276 |
| Защита от изменений папок с установленными компонентами Kaspersky Security для Windows Server ..... | 276 |
| Защита от изменений ключей реестра Kaspersky Security для Windows Server .....                      | 276 |
| Регистрация службы Kaspersky Security как защищенной службы .....                                   | 277 |
| Управление правами доступа к функциям Kaspersky Security для Windows Server .....                   | 278 |
| О правах на управление Kaspersky Security для Windows Server .....                                  | 278 |
| О правах на управление регистрируемыми службами .....                                               | 280 |
| О правах доступа к службе Kaspersky Security Management .....                                       | 281 |
| О правах на управление службой Kaspersky Security .....                                             | 281 |
| Управление правами доступа с помощью Плагина управления .....                                       | 283 |
| Управление правами доступа с помощью Консоли программы .....                                        | 287 |
| Управление правами доступа с помощью Веб-плагина .....                                              | 290 |
| Постоянная защита файлов .....                                                                      | 293 |
| О задаче Постоянная защита файлов .....                                                             | 293 |
| Об области защиты и параметрах безопасности задачи .....                                            | 294 |
| О виртуальной области защиты .....                                                                  | 295 |
| Стандартные области защиты .....                                                                    | 295 |
| Стандартные уровни безопасности .....                                                               | 296 |
| Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов .....                 | 298 |
| Параметры задачи Постоянная защита файлов по умолчанию .....                                        | 300 |
| Управление задачей Постоянная защита файлов с помощью Плагина управления .....                      | 302 |
| Навигация .....                                                                                     | 302 |
| Настройка задачи Постоянная защита файлов .....                                                     | 303 |
| Создание и настройка области защиты задачи .....                                                    | 309 |
| Выбор стандартных уровней безопасности в задаче Постоянная защита файлов .....                      | 310 |
| Настройка параметров безопасности вручную .....                                                     | 310 |
| Управление задачей Постоянная защита файлов с помощью Консоли программы .....                       | 317 |
| Навигация .....                                                                                     | 318 |
| Настройка задачи Постоянная защита файлов .....                                                     | 319 |
| Формирование области защиты .....                                                                   | 324 |
| Настройка параметров безопасности вручную .....                                                     | 328 |
| Статистика задачи Постоянная защита файлов .....                                                    | 336 |
| Управление задачей Постоянная защита файлов с помощью Веб-плагина .....                             | 338 |
| Проверка скриптов .....                                                                             | 343 |
| О задаче Проверка скриптов .....                                                                    | 343 |
| Параметры задачи Проверка скриптов по умолчанию .....                                               | 344 |



|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Настройка параметров задачи Проверка скриптов с помощью Плагина управления ..... | 344 |
| Настройка параметров задачи Проверка скриптов с помощью Консоли программы .....  | 346 |
| Настройка параметров задачи Проверка скриптов с помощью Веб-плагина .....        | 347 |
| Статистика задачи Проверка скриптов .....                                        | 349 |
| Использование KSN .....                                                          | 350 |
| О задаче Использование KSN .....                                                 | 350 |
| Параметры по умолчанию для задачи Использование KSN .....                        | 352 |
| Управление использованием KSN с помощью Плагина управления .....                 | 353 |
| Настройка задачи Использование KSN с помощью Плагина управления .....            | 353 |
| Настройка обработки данных .....                                                 | 355 |
| Управление использованием KSN с помощью Консоли программы .....                  | 357 |
| Настройка задачи Использование KSN с помощью Консоли программы .....             | 358 |
| Настройка обработки данных с помощью Консоли программы .....                     | 359 |
| Управление использованием KSN с помощью Веб-плагина .....                        | 361 |
| Настройка передачи дополнительных данных .....                                   | 364 |
| Статистика задачи Использование KSN .....                                        | 366 |
| Защита трафика .....                                                             | 368 |
| О задаче Защита трафика .....                                                    | 368 |
| О правилах защиты трафика .....                                                  | 369 |
| Защита от почтовых угроз .....                                                   | 370 |
| Список категорий .....                                                           | 371 |
| Параметры стандартных уровней защиты .....                                       | 375 |
| Параметры задачи Защита трафика по умолчанию .....                               | 377 |
| Управление защитой трафика с помощью Плагина управления .....                    | 377 |
| Навигация .....                                                                  | 378 |
| Настройка задачи Защита трафика .....                                            | 379 |
| Настройка антивирусной защиты .....                                              | 384 |
| Настройка защиты от почтовых угроз .....                                         | 387 |
| Настройка обработки веб-адресов и веб-контента .....                             | 388 |
| Настройка веб-контроля .....                                                     | 389 |
| Управление защитой трафика с помощью Консоли программы .....                     | 393 |
| Навигация .....                                                                  | 393 |
| Настройка задачи Защита трафика .....                                            | 394 |
| Настройка антивирусной защиты .....                                              | 399 |
| Настройка защиты от почтовых угроз .....                                         | 402 |
| Настройка обработки веб-адресов и веб-контента .....                             | 403 |
| Настройка веб-контроля .....                                                     | 404 |
| Управление защитой трафика с помощью Веб-плагина .....                           | 408 |

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Защита от шифрования .....                                                   | 409 |
| О задаче Защита от шифрования .....                                          | 409 |
| Статистика задачи Защита от шифрования .....                                 | 410 |
| Параметры по умолчанию для задачи Защита от шифрования .....                 | 411 |
| Настройка задачи Защита от шифрования с помощью Плагина управления .....     | 411 |
| Общие параметры задачи .....                                                 | 412 |
| Формирование области защиты .....                                            | 414 |
| Добавление исключений .....                                                  | 415 |
| Настройка задачи Защита от шифрования с помощью Консоли программы .....      | 416 |
| Общие параметры задачи .....                                                 | 417 |
| Формирование области защиты .....                                            | 418 |
| Добавление исключений .....                                                  | 419 |
| Настройка задачи Защита от шифрования с помощью Веб-плагина .....            | 420 |
| Общие параметры задачи .....                                                 | 420 |
| Формирование области защиты .....                                            | 421 |
| Добавление исключений .....                                                  | 422 |
| Контроль запуска программ .....                                              | 424 |
| О задаче Контроль запуска программ .....                                     | 424 |
| О правилах контроля запуска программ .....                                   | 425 |
| О Контроле пакетов установки .....                                           | 427 |
| Об использовании KSN в задаче Контроль запуска программ .....                | 430 |
| О формировании правил контроля запуска программ .....                        | 431 |
| Параметры по умолчанию для задачи Контроль запуска программ .....            | 433 |
| Управление контролем запуска программ с помощью Плагина управления .....     | 436 |
| Навигация .....                                                              | 436 |
| Настройка параметров задачи Контроль запуска программ .....                  | 438 |
| Настройка Контроля пакетов установки .....                                   | 442 |
| Настройка задачи Формирование правил контроля запуска программ .....         | 444 |
| Настройка правил контроля запуска программ в Kaspersky Security Center ..... | 446 |
| Создание задачи Формирование правил контроля запуска программ .....          | 455 |
| Управление контролем запуска программ с помощью Консоли программы .....      | 460 |
| Навигация .....                                                              | 460 |
| Настройка параметров задачи Контроль запуска программ .....                  | 461 |
| Настройка правил контроля запуска программ .....                             | 468 |
| Настройка задачи Формирование правил контроля запуска программ .....         | 473 |
| Управление контролем запуска программ с помощью веб-плагина .....            | 478 |
| Мониторинг файловых операций .....                                           | 484 |
| О задаче Мониторинг файловых операций .....                                  | 484 |
| О правилах мониторинга файловых операций .....                               | 485 |

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Параметры по умолчанию для задачи Мониторинг файловых операций .....          | 487 |
| Управление мониторингом файловых операций с помощью Плагина управления .....  | 489 |
| Настройка параметров задачи Мониторинг файловых операций.....                 | 489 |
| Настройка правил мониторинга .....                                            | 490 |
| Управление мониторингом файловых операций с помощью Консоли программы .....   | 493 |
| Настройка параметров задачи Мониторинг файловых операций.....                 | 493 |
| Настройка правил мониторинга .....                                            | 494 |
| Управление мониторингом файловых операций с помощью Веб-плагина .....         | 496 |
| Настройка задачи Мониторинг файловых операций.....                            | 496 |
| Настройка правил мониторинга .....                                            | 497 |
| Анализ журналов.....                                                          | 500 |
| О задаче Анализ журналов .....                                                | 500 |
| Параметры по умолчанию для задачи Анализ журналов .....                       | 501 |
| Управление правилами анализа журналов с помощью Плагина управления .....      | 502 |
| Управление стандартными правилами задачи с помощью Плагина управления .....   | 503 |
| Добавление правил анализа журналов с помощью Плагина управления .....         | 504 |
| Управление правилами анализа журналов с помощью Консоли программы .....       | 506 |
| Управление стандартными правилами задачи с помощью Консоли программы .....    | 506 |
| Добавление правил анализа журналов с помощью Консоли программы .....          | 507 |
| Управление правилами анализа журналов с помощью Веб-плагина.....              | 508 |
| Проверка по требованию .....                                                  | 510 |
| О задачах проверки по требованию.....                                         | 510 |
| Об области проверки и параметрах безопасности задачи .....                    | 511 |
| Стандартные области проверки .....                                            | 512 |
| Проверка файлов в облачном хранилище .....                                    | 514 |
| Стандартные уровни безопасности .....                                         | 515 |
| Проверка съемных дисков .....                                                 | 518 |
| О задаче Мониторинг целостности файлов на основе эталона.....                 | 519 |
| Включение запуска задачи проверки по требованию из контекстного меню .....    | 520 |
| Заданные по умолчанию параметры задач проверки по требованию .....            | 521 |
| Управление задачами проверки по требованию с помощью Плагина управления ..... | 523 |
| Навигация .....                                                               | 524 |
| Создание задачи проверки по требованию.....                                   | 525 |
| Настройка области проверки для задачи .....                                   | 530 |
| Выбор стандартных уровней безопасности в задачах проверки по требованию.....  | 531 |
| Настройка параметров безопасности вручную.....                                | 532 |
| Настройка проверки съемных дисков .....                                       | 539 |
| Настройка задачи Мониторинг целостности файлов на основе эталона.....         | 540 |
| Управление задачами проверки по требованию с помощью Консоли программы .....  | 541 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Навигация .....                                                                   | 541 |
| Создание и настройка задачи проверки по требованию .....                          | 542 |
| Область проверки в задачах проверки по требованию .....                           | 544 |
| Настройка параметров безопасности .....                                           | 548 |
| Проверка съемных дисков .....                                                     | 556 |
| Статистика задач проверки по требованию .....                                     | 557 |
| Создание и настройка задачи Мониторинг целостности файлов на основе эталона ..... | 559 |
| Управление задачами проверки по требованию с помощью Веб-плагина .....            | 560 |
| Переход к мастеру создания задачи проверки по требованию .....                    | 560 |
| Переход к свойствам задачи проверки по требованию .....                           | 561 |
| Доверенная зона .....                                                             | 562 |
| О доверенной зоне .....                                                           | 562 |
| Управление доверенной зоной с помощью Плагина управления .....                    | 564 |
| Навигация .....                                                                   | 564 |
| Настройка параметров доверенной зоны с помощью Плагина управления .....           | 565 |
| Управление доверенной зоной с помощью Консоли программы .....                     | 570 |
| Использование доверенной зоны для задач в Консоли программы .....                 | 570 |
| Настройка параметров доверенной зоны в Консоли программы .....                    | 571 |
| Управление доверенной зоной с помощью Веб-плагина .....                           | 576 |
| Защита от эксплойтов .....                                                        | 577 |
| О защите от эксплойтов .....                                                      | 577 |
| Управление защитой от эксплойтов с помощью Плагина управления .....               | 578 |
| Навигация .....                                                                   | 579 |
| Настройка защиты памяти процессов .....                                           | 580 |
| Добавление процесса в область защиты .....                                        | 581 |
| Управление защитой от эксплойтов с помощью Консоли программы .....                | 582 |
| Навигация .....                                                                   | 583 |
| Настройка защиты памяти процессов .....                                           | 583 |
| Добавление процесса в область защиты .....                                        | 584 |
| Управление защитой от эксплойтов с помощью Веб-плагина .....                      | 586 |
| Настройка защиты памяти процессов .....                                           | 586 |
| Добавление процесса в область защиты .....                                        | 587 |
| Техники защиты от эксплойтов .....                                                | 589 |
| Управление иерархическим хранилищем .....                                         | 590 |
| Об иерархическом хранилище .....                                                  | 590 |
| Настройка параметров HSM-системы с помощью Плагина управления .....               | 591 |
| Настройка параметров HSM-системы с помощью Консоли программы .....                | 592 |
| Настройка параметров HSM-системы с помощью Веб-плагина .....                      | 593 |

|                                                                                                               |     |
|---------------------------------------------------------------------------------------------------------------|-----|
| Защита сетевых хранилищ .....                                                                                 | 595 |
| Интеграция Kaspersky Security для Windows Server с сетевыми хранилищами .....                                 | 596 |
| Настройка входящих и исходящих подключений в брандмауэре Windows .....                                        | 597 |
| Настройка параметров безопасности локальных политик в редакторе локальной групповой политики .....            | 598 |
| Работа с Консолью Kaspersky Security для Windows Server .....                                                 | 600 |
| О Консоли Kaspersky Security для Windows Server .....                                                         | 600 |
| Запуск Консоли Kaspersky Security для Windows Server из меню Пуск .....                                       | 601 |
| Окно Консоли Kaspersky Security для Windows Server .....                                                      | 602 |
| Просмотр информации о состоянии защиты сетевых хранилищ .....                                                 | 605 |
| Управление задачами защиты сетевых хранилищ .....                                                             | 607 |
| Защита сетевых хранилищ EMC группы Celerra / VNX .....                                                        | 611 |
| О защите сетевых хранилищ EMC группы Celerra / VNX .....                                                      | 611 |
| Интеграция Kaspersky Security для Windows Server с сетевым хранилищем EMC группы Celerra / VNX .....          | 612 |
| Защита RPC-подключаемых сетевых хранилищ .....                                                                | 613 |
| О защите RPC-подключаемых сетевых хранилищ .....                                                              | 613 |
| О проверке символических ссылок .....                                                                         | 614 |
| О проверке снимков состояния и других томов и папок, доступных только для чтения .....                        | 615 |
| Настройка соединения между RPC-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server .....  | 615 |
| Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ .....                                    | 619 |
| Уровни безопасности в задаче Защита RPC-подключаемых сетевых хранилищ .....                                   | 625 |
| Просмотр статистики задачи Защита RPC-подключаемых сетевых хранилищ .....                                     | 632 |
| Защита ICAP-подключаемых сетевых хранилищ .....                                                               | 634 |
| О защите ICAP-подключаемых сетевых хранилищ .....                                                             | 634 |
| Настройка соединения между ICAP-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server ..... | 635 |
| Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ .....                                   | 636 |
| Уровни безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ .....                                  | 641 |
| Просмотр статистики задачи Защита ICAP-подключаемых сетевых хранилищ .....                                    | 646 |
| Защита от шифрования для NetApp .....                                                                         | 647 |
| О задаче Защита от шифрования для NetApp .....                                                                | 648 |
| Создание и настройка FPolicy .....                                                                            | 649 |
| Настройка Kaspersky Security для Windows Server .....                                                         | 652 |
| Настройка параметров задачи Защита от шифрования для NetApp .....                                             | 655 |
| Управление задачами защиты сетевых хранилищ из Kaspersky Security Center .....                                | 660 |
| Настройка параметров защиты сетевых хранилищ с помощью политик .....                                          | 660 |
| Настройка параметров защиты сетевых хранилищ для одного сервера в Kaspersky Security Center .....             | 662 |

|                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------|-----|
| Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ .....  | 663 |
| Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ ..... | 666 |
| Интеграция со сторонними системами .....                                                                  | 669 |
| Счетчики производительности для программы Системный монитор .....                                         | 669 |
| О счетчиках производительности Kaspersky Security для Windows Server .....                                | 670 |
| Общее количество отвергнутых запросов .....                                                               | 671 |
| Общее количество пропущенных запросов .....                                                               | 672 |
| Количество запросов, не обработанных из-за нехватки системных ресурсов .....                              | 673 |
| Количество запросов, отправленных на обработку .....                                                      | 674 |
| Среднее количество потоков диспетчера файловых перехватов .....                                           | 675 |
| Максимальное количество потоков диспетчера файловых перехватов .....                                      | 676 |
| Количество элементов в очереди зараженных объектов .....                                                  | 677 |
| Количество объектов, обрабатываемых за секунду .....                                                      | 678 |
| Счетчики и ловушки SNMP Kaspersky Security для Windows Server .....                                       | 679 |
| О счетчиках и ловушках SNMP Kaspersky Security для Windows Server .....                                   | 679 |
| SNMP-счетчики Kaspersky Security для Windows Server .....                                                 | 679 |
| SNMP-ловушки Kaspersky Security для Windows Server и их параметры .....                                   | 683 |
| Описания и возможные значения параметров SNMP-ловушек Kaspersky Security для Windows Server .....         | 687 |
| Интеграция с WMI .....                                                                                    | 690 |
| Работа с Kaspersky Security для Windows Server из командной строки .....                                  | 694 |
| Команды .....                                                                                             | 694 |
| Отображение справки о командах Kaspersky Security для Windows Server. KAVSHELL HELP .....                 | 697 |
| Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP .....                         | 697 |
| Проверка выбранной области. KAVSHELL SCAN .....                                                           | 698 |
| Запуск задачи Проверка важных областей. KAVSHELL SCANCritical .....                                       | 702 |
| Управление задачами в асинхронном режиме. KAVSHELL TASK .....                                             | 703 |
| Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG .....                                       | 705 |
| Запуск и остановка задач постоянной защиты сервера. KAVSHELL RTP .....                                    | 705 |
| Управление задачами Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG .....                          | 706 |
| Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE .....                        | 707 |
| Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL .....                             | 709 |
| Запуск задачи Обновление баз программы. KAVSHELL UPDATE .....                                             | 710 |
| Откат обновления баз Kaspersky Security для Windows Server. KAVSHELL ROLLBACK .....                       | 714 |
| Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR .....                                           | 714 |
| Активация программы. KAVSHELL LICENSE .....                                                               | 714 |
| Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE .....                              | 715 |
| Дефрагментация файлов журнала Kaspersky Security для Windows Server. KAVSHELL VACUUM .....                | 718 |

|                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------|-----|
| Очищение базы iSwift. KAVSHELL FBRESET .....                                                              | 719 |
| Включение и выключение создания файла дампа. KAVSHELL DUMP .....                                          | 719 |
| Импорт параметров. KAVSHELL IMPORT .....                                                                  | 720 |
| Экспорт параметров. KAVSHELL EXPORT .....                                                                 | 721 |
| Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO .....                                | 722 |
| Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE .....          | 722 |
| Коды возврата команд .....                                                                                | 725 |
| Коды возврата команд KAVSHELL START и KAVSHELL STOP .....                                                 | 725 |
| Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical .....                                          | 726 |
| Коды возврата команды KAVSHELL TASK LOG-INSPECTOR .....                                                   | 726 |
| Коды возврата команды KAVSHELL TASK .....                                                                 | 727 |
| Коды возврата команды KAVSHELL RTP .....                                                                  | 727 |
| Коды возврата команды KAVSHELL UPDATE .....                                                               | 728 |
| Коды возврата команды KAVSHELL ROLLBACK .....                                                             | 728 |
| Коды возврата команды KAVSHELL LICENSE .....                                                              | 729 |
| Коды возврата команды KAVSHELL TRACE .....                                                                | 729 |
| Коды возврата команды KAVSHELL FBRESET .....                                                              | 730 |
| Коды возврата команды KAVSHELL DUMP .....                                                                 | 730 |
| Коды возврата команды KAVSHELL IMPORT .....                                                               | 731 |
| Коды возврата команды KAVSHELL EXPORT .....                                                               | 731 |
| Коды возврата команды KAVSHELL FIM /BASELINE .....                                                        | 732 |
| Обращение в Службу технической поддержки .....                                                            | 733 |
| Способы получения технической поддержки .....                                                             | 733 |
| Получение технической поддержки по телефону .....                                                         | 733 |
| Техническая поддержка через Kaspersky CompanyAccount .....                                                | 734 |
| Использование файла трассировки и скрипта AVZ .....                                                       | 734 |
| АО "Лаборатория Касперского" .....                                                                        | 736 |
| Информация о стороннем коде .....                                                                         | 738 |
| Уведомления о товарных знаках .....                                                                       | 739 |
| Соответствие терминов .....                                                                               | 740 |
| Глоссарий .....                                                                                           | 741 |
| Приложения .....                                                                                          | 746 |
| Программные компоненты Kaspersky Security для Windows Server и их коды для службы Windows Installer ..... | 746 |
| Программные компоненты Kaspersky Security для Windows Server .....                                        | 746 |
| Программные компоненты набора "Средства администрирования" .....                                          | 749 |
| Процессы Kaspersky Security для Windows Server .....                                                      | 749 |
| Изменения в системе после установки Kaspersky Security для Windows Server .....                           | 750 |

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Параметры установки и удаления и их ключи для службы Windows Installer ..... | 754 |
| Сертифицированное состояние программы: параметры и их значения .....         | 760 |



# Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия «Kaspersky Security для Windows Server 11» (далее также «Kaspersky Security для Windows Server», «программа»).

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security для Windows Server, поддержка организаций, использующих Kaspersky Security для Windows Server, а также специалистам, которые имеют опыт работы с системой удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Security Center.

# Источники информации о Kaspersky Security для Windows Server

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

## В этом разделе

|                                                                                |                    |
|--------------------------------------------------------------------------------|--------------------|
| Источники для самостоятельного поиска информации .....                         | <a href="#">18</a> |
| Обсуждение программ "Лаборатории Касперского" в сообществе пользователей ..... | <a href="#">19</a> |

## Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Security для Windows Server:

- страница Kaspersky Security для Windows Server на веб-сайте "Лаборатории Касперского";
- страница программы на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского" <https://support.kaspersky.ru/>.

Для использования источников информации на веб-сайтах требуется подключение к интернету.

### Страница Kaspersky Security для Windows Server на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security для Windows Server <https://www.kaspersky.ru/business-security/windows-server-security> можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security для Windows Server содержит ссылку на электронный магазин, в котором можно приобрести программу или обновить лицензию.

### Страница Kaspersky Security для Windows Server в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Security для Windows Server в Базе знаний <https://support.kaspersky.ru/ksws10> приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, относящиеся не только к Kaspersky Security для Windows Server, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний могут также включать новости Службы технической поддержки.

### **Документация Kaspersky Security для Windows Server**

В Руководстве администратора Kaspersky Security для Windows Server приведена информация об установке, удалении, настройке и использовании программы.

## **Обсуждение программ "Лаборатории Касперского" в сообществе пользователей**

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями в нашем сообществе <https://community.kaspersky.com/>.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

# О программе

Программное изделие «Kaspersky Security для Windows Server», представляющее собой средство антивирусной защиты типа «Б» второго класса защиты, предназначенное для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Security для Windows Server, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы;
- контроль запуска приложений;
- выполнение проверок сообщений электронной почты (антифишинг);
- контроль выполнения файловых операций;
- защита от эксплойтов;
- контроль загрузки веб-страниц;
- контроль целостности компонентов ОО.

В сертифицированной версии программы не поддерживаются следующие функции:

- контроль устройств;
- защита от сетевых угроз (IDS);
- управление сетевым экраном.

# Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

## Аппаратные и программные требования

В этом разделе описаны аппаратные и программные требования к защищаемым устройствам и сетевым хранилищам.

### В этом разделе

|                                                                                              |                    |
|----------------------------------------------------------------------------------------------|--------------------|
| Требования к серверу, на который устанавливается Kaspersky Security для Windows Server ..... | <a href="#">21</a> |
| Требования к защищаемому сетевому хранилищу .....                                            | <a href="#">23</a> |
| Требования к устройству, на котором устанавливается Консоль программы .....                  | <a href="#">24</a> |

## Требования к серверу, на который устанавливается Kaspersky Security для Windows Server

Перед установкой Kaspersky Security для Windows Server вам нужно удалить с сервера другие антивирусные программы.

Перед установкой Kaspersky Security для Windows Server вам нужно удалить Антивирус Касперского 8.0 для Windows Servers Enterprise Edition. Kaspersky Security для Windows Server можно установить, не удаляя Kaspersky Security 10 для Windows Server.

### Аппаратные требования к серверу

Общие требования:

- x86/64-совместимые одноядерные или многоядерные системы;
- объем дискового пространства:
  - для установки всех программных компонентов: 100 МБ;
  - для загрузки и хранения антивирусных баз: 2 ГБ (рекомендуется);
  - для хранения объектов на карантине и в резервном хранилище: 400 МБ (рекомендуется);
  - для хранения журналов: 1 ГБ (рекомендуется).

Минимальная конфигурация:

- процессор: 1,4 ГГц, одноядерный;
- оперативная память: 1 ГБ;
- диск: 4 ГБ доступного пространства.

Рекомендуемая конфигурация:

- процессор: 2,4 ГГц, четырехъядерный;
- оперативная память: 2 ГБ;
- диск: 4 ГБ доступного пространства.

## Программные требования к серверу

Вы можете установить Kaspersky Security для Windows Server на сервере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и работы Kaspersky Security для Windows Server требуется наличие на сервере установщика Windows версии 3.1.

Вы можете установить Kaspersky Security для Windows Server на сервер под управлением одной из следующих 32-разрядных операционных систем Microsoft Windows:

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

Вы можете установить Kaspersky Security для Windows Server на сервер под управлением одной из следующих 64-разрядных операционных систем Microsoft Windows:

- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;

- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;
- Windows Storage Server 2019;
- Windows Hyper-V Server 2019.

Вы можете установить Консоль Kaspersky Security для Windows Server на следующие типы терминальных серверов:

- Microsoft Remote Desktop Services на базе Windows Server 2008;
- Microsoft Remote Desktop Services на базе Windows Server 2008 R2;
- Microsoft Remote Desktop Services на базе Windows Server 2012;
- Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Microsoft Remote Desktop Services на базе Windows Server 2019;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

Программа Kaspersky Security для Windows Server совместима со следующими версиями Kaspersky Security Center:

- Kaspersky Security Center 10.5;
- Kaspersky Security Center 11;
- Kaspersky Security Center 12.

## Требования к защищаемому сетевому хранилищу

Kaspersky Security для Windows Server может использоваться для защиты следующих сетевых хранилищ:

- NetApp с одной из следующих операционных систем:
  - Data ONTAP 7.x и Data ONTAP 8.x в режиме 7-mode;
  - Data ONTAP 8.2.1 в кластерном режиме;
  - Data ONTAP 9.x (с 9.0 по 9.7) в кластерном режиме.
- Dell™ EMC™ Celerra™ / VNX™ со следующим программным обеспечением:
  - операционная система EMC DART 6.0.36 или выше;
  - Celerra Antivirus Agent (CAVA) 4.5.2.3 или выше.
- Dell EMC Isilon™ с операционной системой OneFS™ 7.0 или выше.
- Hitachi HNAS (ICAP, RPC):
  - 12.0 и выше для интеграции по протоколу ICAP;
  - 11.2 и выше для интеграции по протоколу RPC.
- IBM System Storage серии N.
- Oracle® ZFS Storage Appliance.
- Сетевые хранилища Dell на платформе Dell Compellent™ FS8600:

- FluidFS 6.x.
- FluidFS 5.x.
- HPE 3PAR File Persona 3.3.1:
  - файловый контроллер системы хранения HPE 3PAR STORESERV;
  - системы хранения HPE 3PAR STORESERV 7000с, 8000, 9000, 20000.

## Требования к устройству, на котором устанавливается Консоль программы

### Аппаратные требования к устройству

Рекомендуемый объем оперативной памяти: 128 МБ или более.

Свободное дисковое пространство: 30 МБ.

### Программные требования к устройству

Вы можете установить Консоль программы на устройство с 32-разрядной или 64-разрядной операционной системой Microsoft Windows.

Для установки и работы Консоли программы на устройстве требуется наличие установщика Windows версии 3.1.

Вы можете установить Консоль программы на устройстве под управлением одной из следующих 32-разрядных операционных систем Microsoft Windows:

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10;
- Windows 10 Redstone 1.
- Windows 10 Redstone 2.
- Windows 10 Redstone 3.
- Windows 10 Redstone 4.
- Windows 10 Redstone 5.
- Windows 10 Redstone 6.

Вы можете установить Консоль программы на устройстве под управлением одной из следующих 64-разрядных операционных систем Microsoft Windows:

- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft MultiPoint Server 2011 Standard / Premium;



- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Microsoft MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Storage Server 2019;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10;
- Windows 10 Redstone 1.
- Windows 10 Redstone 2.
- Windows 10 Redstone 3.
- Windows 10 Redstone 4.
- Windows 10 Redstone 5.
- Windows 10 Redstone 6.

## Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе «Аппаратные и программные требования».
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируруемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Должна быть обеспечена возможность периодического контроля целостности ПО программы и БД ПКВ.
16. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
17. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

# Kaspersky Endpoint Agent

Программа Kaspersky Endpoint Agent устанавливается на отдельные устройства в ИТ-инфраструктуре организации. Программа осуществляет постоянный контроль процессов, запущенных на этих устройствах, открытых сетевых соединений и изменяемых файлов. Kaspersky Endpoint Agent поддерживает взаимодействие со следующими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, целевых атак):

- Kaspersky Endpoint Detection and Response Optimum. (Поддерживается Kaspersky Endpoint Agent 3.9 и выше.)

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты ИТ-инфраструктуры организации от сложных кибернетических угроз. Функционал решения сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противостояния сложным атакам, в том числе новым эксплойтам (exploits), программам-шантажистам (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. Решение предназначено для корпоративных пользователей. Дополнительная информация приведена в *онлайн справке Kaspersky Endpoint Detection and Response Optimum*.

- Kaspersky Anti Targeted Attack Platform. (Поддерживается Kaspersky Endpoint Agent 3.8 и выше.)

Kaspersky Anti Targeted Attack Platform – это решение, предназначенное для защиты ИТ-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats. Программа разработана для корпоративных пользователей. Дополнительная информация приведена в *онлайн справке Kaspersky Anti Targeted Attack Platform*.

- Kaspersky Sandbox. (Поддерживается Kaspersky Endpoint Agent 3.7 и выше.)

Kaspersky Sandbox – это решение для обнаружения и блокировки комплексных угроз. Виртуальные образы операционных систем разворачиваются на серверах Kaspersky Sandbox, а проверяемые объекты исполняются внутри этих операционных систем. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки целевых атак. Дополнительная информация приведена в *онлайн справке Kaspersky Sandbox*.

Kaspersky Security 11 для Windows Server поддерживает следующие версии Kaspersky Endpoint Agent: 3.7, 3.8, 3.9.

Дистрибутив Kaspersky Security 11 для Windows Server включает файлы установки для Kaspersky Endpoint Agent 3.9. Вы можете установить Kaspersky Endpoint Agent 3.9 во время установки Kaspersky Security для Windows Server.

# Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.

Определите, какие средства администрирования вы будете использовать для настройки параметров Kaspersky Security для Windows Server и управления им. В качестве средств администрирования Kaspersky Security для Windows Server вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

## Консоль программы

Консоль программы представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Security для Windows Server через Консоль программы, установленную на защищаемом сервере или на другом компьютере в сети организации.

В одну Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток Kaspersky Security для Windows Server, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Security для Windows Server.

Консоль программы входит в набор компонентов "Средства администрирования".

## Утилита командной строки

Вы можете управлять Kaspersky Security для Windows Server из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Security для Windows Server.

## Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации, вы можете управлять Kaspersky Security для Windows Server через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center.** Этот компонент входит в набор программных компонентов Kaspersky Security для Windows Server. Он обеспечивает связь Kaspersky Security для Windows Server с Агентом администрирования. Установите Модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемом сервере.
- **Агент администрирования Kaspersky Security Center.** Установите его на каждом защищаемом сервере. Этот компонент будет обеспечивать взаимодействие между Kaspersky Security для Windows Server, установленным на компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин Kaspersky Security для Windows Server.** Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Security для Windows Server через Сервер администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки плагина, \Server\klcfginst.exe, входит в комплект поставки Kaspersky Security для Windows Server.

# Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Security для Windows Server.

## В этом разделе

|                                                                                                         |                    |
|---------------------------------------------------------------------------------------------------------|--------------------|
| Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows ..... | <a href="#">29</a> |
| Изменения в системе после установки Kaspersky Security для Windows Server .....                         | <a href="#">34</a> |
| Процессы Kaspersky Security для Windows Server .....                                                    | <a href="#">38</a> |
| Параметры установки и удаления и ключи командной строки для службы установщика Windows ..               | <a href="#">38</a> |
| Журналы установки и удаления Kaspersky Security для Windows Server.....                                 | <a href="#">42</a> |
| Планирование установки .....                                                                            | <a href="#">42</a> |
| Установка и удаление программы с помощью мастера.....                                                   | <a href="#">45</a> |
| Установка и удаление программы из командной строки.....                                                 | <a href="#">61</a> |
| Установка и удаление программы с помощью Kaspersky Security Center .....                                | <a href="#">68</a> |
| Установка и удаление программы через групповые политики Active Directory.....                           | <a href="#">73</a> |
| Проверка функций Kaspersky Security для Windows Server. Использование тестового вируса EICAR .....      | <a href="#">76</a> |

## Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows

По умолчанию файлы \server\ks4ws\_x86.msi и \server\ks4ws\_x64.msi предназначены для установки всех компонентов Kaspersky Security для Windows Server. Вы можете установить эти компоненты при выборочной установке программы.

Файлы \client\ks4wstools\_x86.msi и \client\ks4wstools\_x64.msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приведены коды компонентов Kaspersky Security для Windows Server для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Security для Windows Server из командной строки.

## В этом разделе

|                                                                    |                    |
|--------------------------------------------------------------------|--------------------|
| Программные компоненты Kaspersky Security для Windows Server ..... | <a href="#">30</a> |
| Программные компоненты набора Средства администрирования.....      | <a href="#">34</a> |

## Программные компоненты Kaspersky Security для Windows Server

Для установки сертифицированной конфигурации Kaspersky Security для Windows Server необходимо включить установку компонентов Проверка скриптов, Kaspersky Endpoint Agent и Набор счетчиков производительности программы Системный монитор и выключить установку компонентов Контроль устройств, Управление сетевым экраном и Защита от сетевых угроз.

При установке сертифицированной конфигурации Kaspersky Security для Windows Server файл-маркер сертифицированной конфигурации должен находиться в одной папке с установщиком Kaspersky Security для Windows Server.

Защита сетевых хранилищ обеспечивается компонентами Защита RPC-подключаемых сетевых хранилищ, Защита ICAP-подключаемых сетевых хранилищ и Защита от шифрования для NetApp. Установите или снимите флажки напротив данных компонентов при установке сертифицированной конфигурации программы соответствующей типу вашей лицензии.

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Security для Windows Server.

Table 1. Описание программных компонентов Kaspersky Security для Windows Server

| Компонент                 | Код          | Функции компонента                                                                                                                                                                                                                         |
|---------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Основная функциональность | Core         | Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.                                                                                                                                                   |
| Контроль запуска программ | AppCtrl      | Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает запуск в соответствии с заданными правилами контроля запуска программ.<br>Компонент реализуется в задаче Контроль запуска программ.           |
| Защита трафика            | WebGW        | Этот компонент обрабатывает сетевой трафик, включая трафик, поступающий через почтовые серверы, перехватывает и проверяет объекты, передаваемые по веб-трафику, на наличие известных компьютерных и других угроз на защищаемом устройстве. |
| Антивирусная защита       | AVProtection | Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты:<br>Проверка по требованию<br>Постоянная защита файлов                                                                                              |

| Компонент                                | Код           | Функции компонента                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Проверка по требованию                   | Ods           | <p>Этот компонент устанавливает системные файлы Kaspersky Security для Windows Server и выполняет задачи проверки по требованию (проверка объектов защищаемого устройства, выполняемая по команде).</p> <p>Если, устанавливая Kaspersky Security для Windows Server из командной строки, вы укажете другие компоненты Kaspersky Security для Windows Server, не указывая компонент Core, компонент Core будет установлен автоматически.</p> |
| Постоянная защита файлов                 | Oas           | <p>Этот компонент выполняет антивирусную проверку файлов на защищаемом устройстве при обращении к этим файлам.</p> <p>Компонент реализует задачу Постоянная защита файлов.</p>                                                                                                                                                                                                                                                              |
| Защита от шифрования                     | AntiCryptor   | <p>Этот компонент вносит в список заблокированных узлов имена удаленных устройств, проявляющих вредоносную активность.</p> <p>Компонент реализует задачу Защита от шифрования.</p>                                                                                                                                                                                                                                                          |
| Проверка скриптов                        | ScriptChecker | <p>Этот компонент проверяет код скриптов, созданных по технологиям Microsoft Windows. Проверка выполняется при попытке запустить скрипт.</p> <p>Компонент реализует задачу Проверка скриптов.</p>                                                                                                                                                                                                                                           |
| Использование Kaspersky Security Network | Ksn           | <p>Этот компонент обеспечивает защиту на основе облачных технологий "Лаборатории Касперского".</p> <p>Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).</p>                                                                                                                                                                                                     |
| Kaspersky Endpoint Agent                 | Soyuz         | <p>Endpoint Agent обеспечивает взаимодействие клиентского компьютера с решениями "Лаборатории Касперского" для обнаружения комплексных угроз.</p>                                                                                                                                                                                                                                                                                           |

| Компонент                                                               | Код             | Функции компонента                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мониторинг файловых операций                                            | Fim             | Этот компонент позволяет регистрировать операции, производимые над файлами в выбранной области мониторинга.<br>Компонент реализует задачу Мониторинг файловых операций.                                                                                                                                             |
| Защита от эксплойтов                                                    | AntiExploit     | Этот компонент обеспечивает управление параметрами защиты процессов в памяти устройства.                                                                                                                                                                                                                            |
| Модуль интеграции с Агентом администрирования Kaspersky Security Center | AKIntegration   | Этот компонент обеспечивает связь Kaspersky Security для Windows Server с Агентом администрирования Kaspersky Security Center.<br>Вы можете установить этот компонент на защищаемом устройстве, если вы планируете управлять программой через Kaspersky Security Center.                                            |
| Анализ журналов                                                         | LogInspector    | Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.                                                                                                                                                                                                   |
| Защита RPC-подключаемых сетевых хранилищ                                | RPCProt         | Этот компонент защищает RPC-подключаемые сетевые хранилища (например, сетевые хранилища от NetApp) от вирусов и других угроз компьютерной безопасности, проникающих на сервер посредством файлового обмена.                                                                                                         |
| Защита ICAP-подключаемых сетевых хранилищ                               | ICAPProt        | Этот компонент защищает ICAP-подключаемые сетевые хранилища (например, EMC Isilon) от вирусов и других угроз компьютерной безопасности, проникающих на сервер посредством файлового обмена.                                                                                                                         |
| Защита от шифрования для NetApp                                         | AntiCryptorNAS  | Этот компонент защищает папки сетевого хранилища от шифрования. При обнаружении попытки вредоносного шифрования Kaspersky Security для Windows Server блокирует доступ к папкам защищаемого сетевого хранилища.                                                                                                     |
| Набор счетчиков производительности программы Системный монитор          | PerfMonCounters | Компонент устанавливает набор счетчиков производительности программы Системный монитор. Счетчики производительности позволяют измерять производительность Kaspersky Security для Windows Server и находить возможные узкие места при совместной работе Kaspersky Security для Windows Server с другими программами. |



| Компонент                                                          | Код         | Функции компонента                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Поддержка SNMP-протокола                                           | SnmpSupport | Этот компонент публикует счетчики и ловушки Kaspersky Security для Windows Server через Simple Network Management Protocol (протокол SNMP) в Microsoft Windows. Этот компонент можно установить на защищаемое устройство, только если на нем уже установлена служба SNMP.                                                                        |
| Значок Kaspersky Security для Windows Server в области уведомлений | TrayApp     | Компонент отображает значок Kaspersky Security для Windows Server в области уведомлений панели задач защищаемого устройства. Значок Kaspersky Security для Windows Server показывает состояние защиты устройства и позволяет открыть Консоль программы с помощью Microsoft Management Console, если она установлена, и окно <b>О программе</b> . |

## Программные компоненты набора Средства администрирования

В следующей таблице приведены коды и описание программных компонентов набора Средства администрирования.

Table 2. Описание программных компонентов набора Средства администрирования

| Компонент                                      | Код       | Функции компонента                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Оснастка Kaspersky Security для Windows Server | MmcSnapin | Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Security для Windows Server.<br>Если при установке набора "Средства администрирования" из командной строки, вы укажете другие компоненты набора, но не укажете компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически. |
| Help                                           | Help      | Этот компонент представляет собой chm-файл справки. Он сохраняется в папку с файлами Средств администрирования Kaspersky Security для Windows Server. Вы можете открыть файл справки из меню <b>Пуск</b> или с помощью клавиши <b>F1</b> при открытом окне Консоли программы.                                                                |
| Документация                                   | Help      | Kaspersky Security для Windows Server добавляет ярлык для перехода на веб-сайт "Лаборатории Касперского", где документы "Руководство по внедрению для защиты сетевых хранилищ" и "Руководство администратора" доступны в формате PDF. Этот ярлык доступен из меню <b>Пуск</b> .                                                              |

## Изменения в системе после установки Kaspersky Security для Windows Server

При совместной установке Kaspersky Security для Windows Server и набора "Средства администрирования", включающего Консоль программы, служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Security для Windows Server на защищаемом устройстве и на защищаемом устройстве, на котором установлена Консоль программы;
- регистрирует службы Kaspersky Security для Windows Server;
- создает группу пользователей Kaspersky Security для Windows Server;
- регистрирует в системном реестре ключи Kaspersky Security для Windows Server.

Эти изменения описаны ниже.

## Папки Kaspersky Security для Windows Server на защищаемом устройстве

При установке Kaspersky Security для Windows Server на защищаемом устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Security для Windows Server, содержащая исполняемые файлы Kaspersky Security для Windows Server в зависимости от разрядности операционной системы. По умолчанию используются следующие папки установки:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security для Windows Server\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\
- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Security для Windows Server по протоколу SNMP.
  - %Kaspersky Security for Windows Server%\mibs
- 64-разрядные версии исполняемых файлов Kaspersky Security для Windows Server (папка создается только при установке Kaspersky Security для Windows Server в 64-разрядной версии Microsoft Windows).
  - %Kaspersky Security for Windows Server%\x64
- Служебные файлы Kaspersky Security для Windows Server:
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Data\
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Settings\
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Dskm\
- Файлы с параметрами источников обновлений:
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Update\
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Update\
- Обновления баз и программных модулей, загруженные с помощью задачи Копирование обновлений (папка создается при первой загрузке обновлений с помощью задачи Копирование обновлений).
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Update\Distribution\
- Журналы выполнения задач и журнал системного аудита.
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Reports\
- Набор используемых баз данных.
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Bases\Current\
- Резервные копии баз; перезаписываются при каждом обновлении баз.
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Bases\Backup\
- Временные файлы, создаваемые при выполнении задач обновления.
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Bases\Temp\
- Объекты на карантине (папка по умолчанию).
  - %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Quarantine\
- Объекты в резервном хранилище (папка по умолчанию).

%ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Backup\

- Объекты, восстановленные из резервного хранилища и карантина (папка по умолчанию для восстановленных объектов).

%ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\11\Restored\

## Папка, создаваемая при установке Консоли программы

Заданная по умолчанию папка установки Консоли программы, содержащая файлы набора "Средства администрирования", зависит от разрядности операционной системы. По умолчанию используются следующие папки установки:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security для Windows Server Admins Tools\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\

## Службы Kaspersky Security для Windows Server

Следующие службы Kaspersky Security для Windows Server запускаются под системной учетной записью Локальная система (SYSTEM).

- Kaspersky Security Service (KAVFS) – это основная служба Kaspersky Security для Windows Server, которая управляет задачами и рабочими процессами Kaspersky Security для Windows Server.
- Служба Kaspersky Security Management (KAVFSGT) – это служба, предназначенная для управления Kaspersky Security для Windows Server через Консоль программы.
- Служба Kaspersky Security Exploit Prevention (KAVFSSLP) – это служба, исполняющая роль посредника при передаче параметров безопасности внешним агентам безопасности и при получении данных о событиях безопасности.
- Служба Kaspersky Security Script Checker (KAVFSSCS) – это служба, которая запускается совместно с задачей Проверка скриптов и позволяет контролировать выполнение скриптов, созданных с помощью технологий Microsoft Windows.

## Группа Kaspersky Security для Windows Server

KAVWSEE Administrators – это группа на защищаемом устройстве, пользователи которой имеют полный доступ к службе Kaspersky Security Management и ко всем функциям Kaspersky Security для Windows Server.

## Ключи системного реестра

При установке Kaspersky Security для Windows Server создаются следующие ключи системного реестра:

- Свойства Kaspersky Security для Windows Server:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Параметры журнала событий Kaspersky Security для Windows Server (Kaspersky Event Log):  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Свойства службы управления Kaspersky Security для Windows Server:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Параметры счетчиков производительности:
  - В 32-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]

- В 64-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Параметры компонента Поддержка SNMP-протокола:
  - В 32-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\11\SnmpAgent]
  - В 64-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\SnmpAgent]
- Параметры файла дампа:
  - В 32-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\11\CrashDump]
  - В 64-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\CrashDump]
- Параметры файла трассировки:
  - В 32-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\11\Trace]
  - В 64-х разрядной версии Microsoft Windows:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\Trace]
- Параметры задач и функций программы:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\Environment]

## Процессы Kaspersky Security для Windows Server

Kaspersky Security для Windows Server запускает процессы, описанные в таблице ниже.

Table 3. Процессы Kaspersky Security для Windows Server

| Имя файла    | Назначение                                                          |
|--------------|---------------------------------------------------------------------|
| kavfswp.exe  | Рабочий процесс Kaspersky Security для Windows Server               |
| kavtray.exe  | Процесс значка области уведомлений                                  |
| kavfsmui.exe | Процесс компонента Диагностическое окно                             |
| kavshell.exe | Процесс утилиты командной строки                                    |
| kavfsrcn.exe | Процесс удаленного управления Kaspersky Security для Windows Server |
| kavfs.exe    | Процесс службы Kaspersky Security                                   |
| kavfsgt.exe  | Процесс службы Kaspersky Security Management                        |
| kavfswh.exe  | Процесс службы Kaspersky Security Exploit Prevention                |
| kavfsscs.exe | Служба Kaspersky Security Script Checker                            |

## Параметры установки и удаления и ключи командной строки для службы установщика Windows

В этом разделе описаны параметры установки и удаления Kaspersky Security для Windows Server, их значения по умолчанию, указаны ключи для изменения параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Security для Windows Server из командной строки.

### Параметры установки и ключи командной строки для установщика Windows

- Согласие с условиями Лицензионного соглашения: необходимо принять условия для установки Kaspersky Security для Windows Server.

Возможны следующие значения ключа командной строки `EULA=<значение>`:

- 0 – вы отклоняете условия Лицензионного соглашения (значение по умолчанию).
- 1 – вы принимаете условия Лицензионного соглашения.
- Согласие с условиями Политики конфиденциальности: необходимо принять условия для установки Kaspersky Security для Windows Server.

Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<значение>`:

- 0 – вы отклоняете условия Политики конфиденциальности (значение по умолчанию).
- 1 – вы принимаете условия Политики конфиденциальности.
- Разрешить установку Kaspersky Security для Windows Server, если не установлено обновление KB4528760. Дополнительная информация об обновлении KB4528760 приведена на веб-сайте Microsoft <https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760>.

Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<значение>`:

- 0 – отменить установку Kaspersky Security для Windows Server, если не установлено обновление KB4528760 (значение по умолчанию).
- 1 – разрешить установку Kaspersky Security для Windows Server, если не установлено обновление KB4528760.

Обновление KB4528760 исправляет уязвимость безопасности CVE-2020-0601. Дополнительная информация об уязвимости в системе безопасности CVE-2020-0601 приведена на веб-сайте Microsoft <https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760>.

- Установка Kaspersky Security для Windows Server с предварительной проверкой активных процессов и загрузочных секторов локальных дисков.

Возможны следующие значения ключа командной строки `PRESCAN=<значение>`:

- 0 – не выполнять предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки (значение по умолчанию).
- 1 – выполнить предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки.
- Папка, в которую будут сохранены файлы Kaspersky Security для Windows Server при установке. Вы можете указать другую папку.

Значение по умолчанию для ключа командной строки `INSTALLDIR=<полный путь к папке>`:

- Kaspersky Security для Windows Server: %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server
- Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools
- В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%
- Задача Постоянная защита файлов запускается сразу после запуска Kaspersky Security для Windows Server. Включите этот параметр, чтобы запускать Постоянную защиту файлов и Проверку скриптов при запуске Kaspersky Security для Windows Server (рекомендуется).

Возможны следующие значения ключа командной строки `RUNRTP=<значение>`:

- 1 – запустить (значение по умолчанию).
- 0 – не запускать.
- Исключения из области защиты, рекомендуемые корпорацией Microsoft. В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать корпорация Microsoft. Некоторые программы на защищаемом устройстве могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, используемые этими программами. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.



Возможны следующие значения ключа командной строки `ADDMSEXCLUSION=<значение>`:

- 1 – исключить (значение по умолчанию).
- 0 – не исключать.
- Объекты, исключаемые из области защиты в соответствии с рекомендациями "Лаборатории Касперского". В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать "Лаборатория Касперского".

Возможны следующие значения ключа командной строки `ADDKLEXCLUSION=<значение>`:

- 1 – исключить (значение по умолчанию).
- 0 – не исключать.
- Разрешить удаленное подключение к Консоли программы По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом устройстве, не разрешено. Во время установки можно разрешить подключение. Kaspersky Security для Windows Server создаст разрешающие правила для процесса `kavfsgt.exe` по протоколу TCP для всех портов.

Возможны следующие значения ключа командной строки `ALLOWREMOTECON=<значение>`:

- 1 – разрешить.
- 0 – запретить (значение по умолчанию).
- Путь к файлу ключа (`LICENSEKEYPATH`). По умолчанию установщик Windows пытается найти файл с расширением `.key` в папке `\server` комплекта поставки. Если в папке `\server` имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Вы можете предварительно сохранить файл ключа в папке `\server` или указать другой путь к файлу ключа с помощью параметра **Добавление ключа**. Вы можете добавить ключ после установки Kaspersky Security для Windows Server с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ во время установки программы, после установки Kaspersky Security для Windows Server не будет функционировать.
- Путь к конфигурационному файлу. Kaspersky Security для Windows Server импортирует параметры из указанного конфигурационного файла, созданного в программе. Kaspersky Security для Windows Server не импортирует из конфигурационного файла пароли, например пароли учетных записей для запуска задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.

Значение по умолчанию для параметра `CONFIGPATH=<имя конфигурационного файла>` не указано.

- Параметр включения сетевых соединений для Консоли программы используется для установки Консоли Kaspersky Security для Windows Server на другое устройство. Вы можете удаленно управлять защитой устройства с другого устройства, на котором установлена Консоль Kaspersky Security для Windows Server. В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла `kavfsrcn.exe` для удаленного управления Kaspersky Security для Windows Server и предоставлен доступ к DCOM-программам. После завершения установки добавьте пользователей в группу KAVWSEE Administrators, чтобы разрешить им управлять программой удаленно, если на защищаемом устройстве установлена операционная система Microsoft Windows Server 2008, а также разрешите на защищаемом устройстве сетевые подключения к службе Kaspersky Security Management (файл `kavfsgt.exe`). Можно более детально ознакомиться с дополнительной настройкой при установке Консоли Kaspersky Security для Windows



Server на другое устройство (см. раздел "Дополнительная настройка после установки Консоли программы на другое устройство" на стр. [51](#)).

Возможны следующие значения ключа командной строки `ADDWFEXCLUSION=<значение>`:

- 1 – разрешить.
- 0 – запретить (значение по умолчанию).
- Отключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или выключить проверку на наличие несовместимого программного обеспечения при установке программы на защищаемое устройство в фоновом режиме. Независимо от значения этого параметра, при установке Kaspersky Security для Windows Server программа всегда предупреждает о других версиях программы, установленных на этом защищаемом устройстве.

Возможны следующие значения ключа командной строки `SKIPINCOMPATIBLESW=<значение>`:

- 0 – выполняется проверка на несовместимое программное обеспечение (значение по умолчанию).
- 1 – проверка на наличие несовместимого программного обеспечения не выполняется.

## Параметры удаления и ключи командной строки для установщика Windows

- Восстановление содержимого карантина.

Возможны следующие значения ключа командной строки `RESTOREQTN=<значение>`:

- 0 – удалить содержимое карантина (значение по умолчанию).
- 1 – восстановить содержимое карантина в папку, указанную в качестве значения параметра `RESTOREPATH`, во вложенную подпапку `\Quarantine`.
- Восстановление содержимого резервного хранилища.

Возможны следующие значения ключа командной строки `RESTOREBCK=<значение>`:

- 0 – удалить содержимое резервного хранилища (значение по умолчанию).
- 1 – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра `RESTOREPATH`, во вложенную папку `\Backup`.
- Ввод текущего пароля для подтверждения операции удаления (при включенной функции защиты паролем).

Значение по умолчанию для ключа `UNLOCK_PASSWORD=<указанный пароль>` не задано.

- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

Значение по умолчанию для ключа командной строки `RESTOREPATH=<полный путь к папке>` – `%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\11\Restored`.

## Журналы установки и удаления Kaspersky Security для Windows Server

Если вы выполняете установку или удаление Kaspersky Security для Windows Server с помощью мастера установки (удаления), служба установщика Windows создает журнал установки (удаления). Файл журнала с именем ks4ws\_v11\_install\_<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала) сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление** для Консоли программы или для Kaspersky Security для Windows Server, в папке %temp% будет автоматически создан файл журнала с именем ks4ws\_11\_maintenance.log.

Если вы выполняете установку или удаление Kaspersky Security для Windows Server из командной строки, по умолчанию файл журнала установки не создается.

► Чтобы установить Kaspersky Security для Windows Server и создать файл журнала на диске C:\, выполните одну из следующих команд:

- `msiexec /i ks4ws_x86.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`

## Планирование установки

В этом разделе описаны средства администрирования Kaspersky Security для Windows Server, особенности установки и удаления Kaspersky Security для Windows Server с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. [45](#)), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. [61](#)), с помощью Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. [68](#)) и через групповые политики Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. [73](#)).

Перед началом установки Kaspersky Security для Windows Server составьте план основных этапов установки.

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Security для Windows Server и для настройки программы.
2. Определите, какие программные компоненты требуется установить (см. раздел "Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows" на стр. [29](#)).
3. Выберите способ установки.

### В этом разделе

|                                       |                    |
|---------------------------------------|--------------------|
| Выбор средств администрирования ..... | <a href="#">43</a> |
| Выбор способа установки .....         | <a href="#">44</a> |

## Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров и управления Kaspersky Security для Windows Server. В качестве средств администрирования Kaspersky Security для Windows Server вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

### Консоль Kaspersky Security для Windows Server

Консоль Kaspersky Security для Windows Server представляет собой самостоятельную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Security для Windows Server через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

Вы можете добавить несколько оснасток Kaspersky Security для Windows Server в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Security для Windows Server.

Консоль программы входит в набор компонентов "Средства администрирования".

### Утилита командной строки

Вы можете управлять Kaspersky Security для Windows Server из командной строки защищаемого устройства.

Утилита командной строки входит в набор программных компонентов Kaspersky Security для Windows Server.

### Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств в вашей организации, вы можете управлять Kaspersky Security для Windows Server через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center.** Этот компонент входит в группу программных компонентов Kaspersky Security для Windows Server. Он позволяет Kaspersky Security для Windows Server взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемое устройство.
- **Агент администрирования Kaspersky Security Center.** Установите его на каждое защищаемое устройство. Этот компонент будет обеспечивать взаимодействие между программой Kaspersky Security для Windows Server, установленной на защищаемом устройстве, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин управления Kaspersky Security для Windows Server.** Дополнительно на управляемом устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Security для Windows Server для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления, `server\klcfginst.exe`, входит в комплект поставки Kaspersky Security для Windows Server.

## Выбор способа установки

После определения программных компонентов для установки Kaspersky Security для Windows Server (см. раздел "Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows" на стр. [29](#)) необходимо выбрать способ установки программы.

Выберите способ установки в зависимости от архитектуры сети и следующих условий:

- Потребуется ли вам задать специальные параметры установки Kaspersky Security для Windows Server или вы будете использовать рекомендуемые параметры установки (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. [38](#)).
- Будут ли параметры установки едиными для всех защищаемых устройств или индивидуальными для каждого защищаемого устройства.

Вы можете установить Kaspersky Security для Windows Server как с помощью мастера установки, так и в режиме без взаимодействия с пользователем, указав параметры установки в командной строке. Вы можете выполнить централизованную удаленную установку Kaspersky Security для Windows Server: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить и настроить Kaspersky Security для Windows Server на отдельном защищаемом устройстве и сохранить его параметры в конфигурационный файл, чтобы затем использовать созданный файл для установки Kaspersky Security для Windows Server на другие защищаемые устройства. Однако это невозможно при установке программы через групповые политики Active Directory.

### Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Security для Windows Server (см. раздел "Программные компоненты Kaspersky Security для Windows Server" на стр. [30](#)) из файла \server\setup.exe, входящего в комплект поставки, на защищаемом устройстве.
- Консоль Kaspersky Security для Windows Server (см. раздел "Установка Консоли Kaspersky Security для Windows Server" на стр. [49](#)) из файла \client\setup.exe, входящего в комплект поставки, на защищаемом устройстве или другом устройстве в локальной сети.

### Запуск из командной строки файла пакета установки с параметрами установки

Запустив файл пакета установки без ключей, вы установите Kaspersky Security для Windows Server с параметрами установки по умолчанию. С помощью ключей Kaspersky Security для Windows Server вы можете изменять параметры установки.

Вы можете установить Консоль программы на защищаемом устройстве или на рабочем месте администратора.

Вы также можете использовать команды для установки Kaspersky Security для Windows Server и Консоли программы (см. раздел "Установка и удаление программы из командной строки" на стр. [61](#)).

### Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой устройств в сети, вы можете установить Kaspersky Security для Windows Server на несколько устройств с помощью задачи удаленной установки.

Защищаемые устройства, на которых вы хотите установить Kaspersky Security для Windows Server с помощью Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. [68](#)), могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене, а также вообще не принадлежать ни к одному домену.

## Централизованная установка через групповые политики Active Directory

С помощью групповых политик Active Directory вы можете устанавливать Kaspersky Security для Windows Server на защищаемом устройстве. Вы можете установить Консоль программы на защищаемом устройстве или рабочем месте администратора.

Вы можете установить Kaspersky Security для Windows Server, используя только параметры установки по умолчанию.

Защищаемые устройства, на которых программа Kaspersky Security для Windows Server была установлена с помощью групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. [73](#)), должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске защищаемого устройства, перед входом в Microsoft Windows.

## Установка и удаление программы с помощью мастера

В этом разделе описана установка и удаление Kaspersky Security для Windows Server и Консоли программы с помощью мастера установки, а также приведена информация о дополнительных параметрах Kaspersky Security для Windows Server и действиях при установке.

### В этом разделе

|                                                                                            |                    |
|--------------------------------------------------------------------------------------------|--------------------|
| Установка с помощью мастера установки .....                                                | <a href="#">45</a> |
| Изменение состава компонентов и восстановление Kaspersky Security для Windows Server ..... | <a href="#">57</a> |
| Удаление с помощью мастера установки.....                                                  | <a href="#">58</a> |

## Установка с помощью мастера установки

В следующих разделах содержится информация об установке Kaspersky Security для Windows Server, Консоли программы и расширения для Microsoft Outlook.

► *Чтобы установить и начать использовать Kaspersky Security для Windows Server, выполните следующие действия:*

1. Установите Kaspersky Security для Windows Server на защищаемое устройство.
2. На устройства, с которых вы планируете управлять Kaspersky Security для Windows Server, установите Консоль программы.
3. Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку, чтобы пользователи Консоли программы могли удаленно управлять Kaspersky Security для Windows Server.
4. Установите расширение для Microsoft Outlook на устройство, на котором установлен клиент Microsoft Outlook.
5. Выполните действия после установки Kaspersky Security для Windows Server.

## В этом разделе

|                                                                                       |                    |
|---------------------------------------------------------------------------------------|--------------------|
| Установка Kaspersky Security для Windows Server .....                                 | <a href="#">46</a> |
| Установка Консоли Kaspersky Security для Windows Server .....                         | <a href="#">49</a> |
| Установка расширения Kaspersky Security для Microsoft Outlook .....                   | <a href="#">50</a> |
| Дополнительная настройка после установки Консоли программы на другое устройство ..... | <a href="#">51</a> |
| Действия после установки Kaspersky Security для Windows Server .....                  | <a href="#">54</a> |

## Установка Kaspersky Security для Windows Server

Для установки сертифицированной конфигурации Kaspersky Security для Windows Server необходимо включить установку компонентов Проверка скриптов, Kaspersky Endpoint Agent и Набор счетчиков производительности программы Системный монитор и выключить установку компонентов Контроль устройств, Управление сетевым экраном и Защита от сетевых угроз.

При установке сертифицированной конфигурации Kaspersky Security для Windows Server файл-маркер сертифицированной конфигурации должен находиться в одной папке с установщиком Kaspersky Security для Windows Server.

Защита сетевых хранилищ обеспечивается компонентами Защита RPC-подключаемых сетевых хранилищ, Защита ICAP-подключаемых сетевых хранилищ и Защита от шифрования для NetApp. Установите или снимите флажки напротив данных компонентов при установке сертифицированной конфигурации программы соответствующей типу вашей лицензии.

Перед установкой Kaspersky Security для Windows Server выполните следующие действия:

Убедитесь, что на защищаемом устройстве не установлены другие антивирусные программы. Вам нужно удалить Антивирус Касперского 8.0 для Windows Servers Enterprise Edition. Kaspersky Security для Windows Server можно установить, не удаляя Kaspersky Security 10 для Windows Server.

- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом устройстве.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Security для Windows Server. Вы можете прервать установку Kaspersky Security для Windows Server на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Подробная информация о параметрах установки и удаления приведена в разделе "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. [38](#).

- Чтобы установить Kaspersky Security для Windows Server с помощью мастера установки, выполните следующие действия:

1. На защищаемом устройстве запустите файл setup.exe.
2. В открывшемся окне в разделе **Установка** перейдите по ссылке **Установить Kaspersky Security для Windows Server**.
3. В открывшемся окне приветствия мастера установки Kaspersky Security для Windows Server нажмите на кнопку **Далее**.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения и Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности**.

Если вы не принимаете Лицензионное соглашение и Политику конфиденциальности, установка будет прервана.

6. Нажмите на кнопку **Далее**.

Если на защищаемом устройстве уже установлена совместимая версия программы, откроется окно **Обнаружена предыдущая версия программы**.

Если на сервере не обнаружены предыдущие версии программы, перейдите к шагу 8 инструкции.

7. Чтобы обновить предыдущую версию программы, нажмите на кнопку **Установить**. С помощью мастера установки программа будет обновлена до Kaspersky Security для Windows Server 11. Совместимые параметры будут сохранены в новой версии. По завершении обновления откроется окно мастера **Установка завершена** (перейдите к шагу 15 инструкции).

Откроется окно **Быстрая проверка перед началом установки**.

8. В окне **Быстрая проверка перед началом установки** установите флажок **Проверить компьютер на вирусы**, чтобы проверить на наличие угроз системную память и загрузочные секторы локальных дисков защищаемого устройства. Нажмите на кнопку **Далее**. По окончании проверки откроется окно с результатами проверки.

В окне содержится информация о проверенных объектах на управляемом устройстве: общее количество проверенных объектов, количество обнаруженных угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или потенциально опасных процессов, которые программа Kaspersky Security для Windows Server удалила из памяти, и количество опасных или потенциально опасных процессов, которые программе не удалось удалить.

Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

9. В окне **Быстрая проверка перед началом установки** нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

10. Выберите компоненты, которые вы хотите установить.



По умолчанию все компоненты Kaspersky Security для Windows Server включены в список рекомендуемых к установке, за исключением компонента Проверка скриптов.

Компонент Поддержка SNMP-протокола Kaspersky Security для Windows Server отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба Microsoft Windows SNMP.

Если вы выбрали установку Kaspersky Endpoint Agent (см. стр. [27](#)), на следующем шаге мастера откроется окно **Лицензионное соглашение Kaspersky Endpoint Agent**. Если вы принимаете условия и положения Лицензионного соглашения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения**. Установка Kaspersky Endpoint Agent начнется после установки Kaspersky Security для Windows Server.

11. Чтобы отменить все изменения, в окне **Выборочная установка** нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.
12. В окне **Выбор папки назначения** выполните следующие действия:
  - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Security для Windows Server.
  - Если требуется, нажмите на кнопку **Диск** для просмотра информации о доступном пространстве на локальных жестких дисках.Нажмите на кнопку **Далее**.
13. В окне **Дополнительные параметры установки** настройте следующие параметры установки:
  - **Включить постоянную защиту после установки программы**
  - **Добавить к исключениям файлы, рекомендованные Microsoft**
  - **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**Нажмите на кнопку **Далее**.
14. В окне **Импорт параметров из конфигурационного файла** выполните следующие действия:
  - a. Если вы хотите импортировать параметры Kaspersky Security для Windows Server из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.
  - b. Нажмите на кнопку **Далее**.
15. В окне **Активация программы** выполните одно из следующих действий:
  - Если вы хотите активировать программу, укажите файл ключа Kaspersky Security для Windows Server для активации программы.
  - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
  - Если вы предварительно сохранили файл ключа в папке \server комплекта поставки, имя этого файла отобразится в поле **Ключ**.
  - Чтобы добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.



Мастер установки не позволяет активировать программу с помощью кода активации. Если вы хотите активировать программу с помощью кода активации, его можно указать после установки программы.

После добавления файла ключа в окне отобразится информация о лицензии. В Kaspersky Security для Windows Server отображается расчетная дата истечения срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, а истекает не позднее даты окончания срока действия файла ключа.

Нажмите на кнопку **Далее**, чтобы добавить файл ключа в программу.

16. В окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Security для Windows Server.
17. По завершении установки откроется окно **Установка завершена**.
18. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о версии после завершения работы мастера установки.
19. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. По завершении установки программа Kaspersky Security для Windows Server готова к работе, если вы добавили ключ активации.

## Установка Консоли Kaspersky Security для Windows Server

Следуя инструкциям мастера установки, настройте параметры установки Консоли программы. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

► Чтобы установить Консоль программы, выполните следующие действия:

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.
2. На защищаемом устройстве запустите файл setup.exe.  
Откроется окно программы-приветствия.
3. Перейдите по ссылке **Установить Консоль Kaspersky Security для Windows Server**.  
Откроется окно приветствия мастера установки.
4. Нажмите на кнопку **Далее**.
5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и, чтобы продолжить установку, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.
6. Нажмите на кнопку **Далее**.  
Откроется окно **Дополнительные параметры установки**.
7. В окне **Дополнительные параметры установки** выполните следующие действия:
  - Если вы планируете с помощью Консоли программы управлять программой Kaspersky Security для Windows Server, установленной на удаленном устройстве, установите флажок **Разрешить удаленный доступ**.

- Чтобы открыть окно **Выборочная установка** и выбрать компоненты, выполните следующие действия:
  - a. Нажмите на кнопку **Дополнительно**.  
Откроется окно **Выборочная установка**.
  - b. В списке выберите набор компонентов "Средства администрирования".  
По умолчанию устанавливаются все компоненты.
  - c. Нажмите на кнопку **Далее**.

Подробная информация о компонентах Kaspersky Security для Windows Server приведена в разделе "Коды программных компонентов Kaspersky Security для Windows Server для службы установщика Windows" на стр. [29](#).

8. В окне **Выбор папки назначения** выполните следующие действия:
  - a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
  - b. Нажмите на кнопку **Далее**.
9. В окне **Готовность к установке** нажмите на кнопку **Установить**.  
Мастер приступит к установке выбранных компонентов.
10. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. Консоль программы будет установлена на защищаемом устройстве.

Если вы установили набор "Средства администрирования" не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли программы на другом устройстве" на стр. [51](#)).

## Установка расширения Kaspersky Security для Microsoft Outlook

Следуйте инструкциям Мастера установки для настройки параметров установки расширения для Microsoft Outlook. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Вы можете установить расширение для Microsoft Outlook на защищаемое устройство, только если на нем установлены Kaspersky Security для Windows Server и почтовый клиент Microsoft Outlook.

- Чтобы установить расширение для Microsoft Outlook, выполните следующие действия:
1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.
  2. На защищаемом устройстве запустите файл setup.exe.  
Откроется окно программы-приветствия.
  3. Перейдите по ссылке **Установить расширение Kaspersky Security 11 для Microsoft Outlook (x86)** или **Установить расширение Kaspersky Security 11 для Microsoft Outlook (x64)**, в зависимости от разрядности установленного клиента Microsoft Outlook.

Откроется окно приветствия мастера установки.

4. Нажмите на кнопку **Далее**.

5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и, чтобы продолжить установку, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

6. Нажмите на кнопку **Далее**.

Откроется окно **Папка назначения**.

7. В открывшемся окне **Папка назначения** выполните следующие действия:

- Если вы хотите изменить папку назначения, нажмите на кнопку **Изменить**.

Откроется окно **Изменить папку назначения**.

а. Укажите нужную папку назначения.

б. Нажмите на кнопку **ОК**.

- Если вы не хотите менять папку назначения, нажмите на кнопку **Далее**.

Откроется окно **Готовность к установке расширения Kaspersky Security для Windows Server 11 для Microsoft Outlook**.

8. В окне **Готовность к установке** нажмите на кнопку **Установить**.

Мастер приступит к установке выбранных компонентов.

9. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена.

Если во время установки расширения был запущен почтовый клиент Microsoft Outlook, перезапустите его после завершения установки.

## Дополнительная настройка после установки Консоли программы на другое устройство

Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните следующие действия для того, чтобы пользователи могли удаленно управлять Kaspersky Security для Windows Server:

- На защищаемом устройстве добавьте пользователей Kaspersky Security для Windows Server в группу KAVWSEE Administrators.
- Включите сетевые соединения для службы Kaspersky Security Management (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. [281](#)), если на защищаемом устройстве используется брандмауэр Windows или сетевой экран стороннего поставщика.
- Если во время установки Консоли программы на устройство под управлением Microsoft Windows не был установлен флажок **Разрешить удаленный доступ**, вручную включите сетевые соединения для Консоли программы через сетевой экран устройства.

Консоль программы на удаленном устройстве использует протокол DCOM для получения информации о событиях Kaspersky Security для Windows Server, например, о проверенных объектах или о завершении задач, от службы Kaspersky Security Management на защищаемом устройстве. Необходимо разрешить

сетевые соединения для Консоли программы в параметрах брандмауэра Windows, чтобы устанавливать соединения между Консолью программы и службой Kaspersky Security Management.

На удаленном устройстве, на котором установлена Консоль программы, выполните следующие действия:

- Убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM).
- В параметрах брандмауэра Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Security для Windows Server – kavfsrscn.exe.

Устройство, на котором установлена Консоль программы, обменивается информацией с защищаемым устройством через порт TCP 135.

- Чтобы разрешить подключение, настройте правило исходящего подключения для брандмауэра Windows.  
В отличие от стандартных служб TCP/IP и UDP/IP, где для каждого протокола имеется фиксированный порт, DCOM динамически назначает порты удаленным COM-объектам. Если между клиентским устройством (на котором установлена Консоль программы) и DCOM-устройством (защищаемым устройством) находится сетевой экран, нужно открыть широкий диапазон портов.

Аналогичные шаги следует выполнить для настройки любого другого программного или аппаратного сетевого экрана.

► Если Консоль программы открыта во время настройки соединения между защищаемым устройством и устройством, на котором установлена Консоль программы, выполните следующие действия:

1. Закройте Консоль программы.
  2. Дождитесь завершения процесса удаленного управления Kaspersky Security для Windows Server – kavfsrscn.exe.
  3. Перезапустите Консоль программы.
- Будут применены новые параметры соединения.

В этом разделе

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Разрешение анонимного удаленного доступа к программам COM .....                                             | 52 |
| Разрешение сетевых соединений для процесса удаленного управления Kaspersky Security для Windows Server..... | 53 |
| Добавление правила исходящего подключения для брандмауэра Windows .....                                     | 54 |

Разрешение анонимного удаленного доступа к программам COM

Названия параметров могут отличаться в разных операционных системах Windows.

- Чтобы разрешить анонимный удаленный доступ к программам COM, выполните следующие действия:

1. На удаленном устройстве, на котором установлена Консоль Kaspersky Security для Windows Server, откройте консоль Службы компонентов.
2. Выберите **Пуск → Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **ОК**.
5. В консоли **Службы компонентов** защищаемого устройства разверните узел **Компьютеры**.
6. Откройте контекстное меню узла **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в блоке параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.
10. Нажмите на кнопку **ОК**.

## Разрешение сетевых соединений для процесса удаленного управления Kaspersky Security для Windows Server

Названия параметров могут отличаться в разных операционных системах Windows.

- Чтобы открыть TCP-порт 135 в брандмауэре Windows и разрешить сетевые соединения для процесса удаленного управления Kaspersky Security для Windows Server, выполните следующие действия:
1. На удаленном устройстве закройте Консоль Kaspersky Security для Windows Server.
  2. Выберите **Пуск > Панель управления > Брандмауэр Windows**.
  3. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
  4. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.
  5. В окне **Добавление программы** укажите файл `kavfsrcn.exe`. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Security для Windows Server с помощью Microsoft Management Console.
  6. Нажмите на кнопку **ОК**.
  7. Нажмите на кнопку **ОК** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

## Добавление правила исходящего подключения для брандмауэра Windows

Названия параметров могут отличаться в разных операционных системах Windows.

- Чтобы добавить правило исходящего подключения для брандмауэра Windows, выполните следующие действия:
1. Выберите **Пуск > Панель управления > Брандмауэр Windows**.
  2. В окне **Брандмауэр Windows** перейдите по ссылке **Дополнительные параметры**.  
Откроется окно **Брандмауэр Windows в режиме повышенной безопасности**.
  3. Выберите вложенный узел **Правила для исходящего подключения**.
  4. На панели **Действия** выберите пункт **Создать правило**.
  5. В открывшемся окне **Мастер создания правила для нового исходящего подключения** выберите параметр **Порт** и нажмите на кнопку **Далее**.
  6. Выберите протокол **TCP**.
  7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.
  8. В окне **Действие** выберите пункт **Разрешить подключение**.
  9. Сохраните созданное правило и закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Брандмауэр Windows не разрешает установку сетевых соединений между Консолью программы и службой Kaspersky Security Management.

## Действия после установки Kaspersky Security для Windows Server

Kaspersky Security для Windows Server запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Security для Windows Server был установлен флажок **Включить постоянную защиту после установки программы** (по умолчанию), программа проверяет объекты файловой системы устройства при доступе к ним. Если при выборочной установке был установлен компонент Проверка скриптов, Kaspersky Security для Windows Server будет выполнять проверку программного кода всех скриптов при их запуске. Каждую пятницу в 20:00 Kaspersky Security для Windows Server выполняет задачу Проверка важных областей.

После установки Kaspersky Security для Windows Server рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз программы. После установки Kaspersky Security для Windows Server проверяет объекты с использованием баз, которые входили в состав программы при поставке.

Рекомендуется сразу же обновить базы Kaspersky Security для Windows Server, так как базы могли устареть.

Далее программа будет обновлять базы каждый час согласно расписанию, установленному в задаче по умолчанию.

- Выполнить Проверку важных областей, если перед установкой Kaspersky Security для Windows Server на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Security для Windows Server.

## В этом разделе

|                                                          |    |
|----------------------------------------------------------|----|
| Запуск и настройка задачи Обновление баз программы ..... | 55 |
| Проверка важных областей .....                           | 57 |

## Запуск и настройка задачи Обновление баз программы

► Чтобы обновить базы программы после установки, выполните следующие действия:

1. В свойствах задачи обновления баз программы настройте соединение с источником обновлений – HTTP- или FTP-серверами обновлений "Лаборатории Касперского".
2. Запустите задачу Обновление баз программы.

В вашей сети может быть не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети. В этом случае может потребоваться проверка подлинности при доступе к прокси-серверу.

► Чтобы указать дополнительные параметры прокси-сервера и параметры проверки подлинности для доступа к прокси-серверу, выполните следующие действия:

1. Откройте контекстное меню узла **Kaspersky Security**.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры программы**.
3. Выберите закладку **Параметры соединения**.
4. В разделе **Параметры прокси-сервера** установите флажок **Использовать параметры указанного прокси-сервера**.
5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.
6. В разделе **Параметры аутентификации прокси-сервера** выберите требуемый метод аутентификации из раскрывающегося списка:
  - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Security для Windows Server будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи. По умолчанию задача запускается под учетной записью **Локальная система (SYSTEM)**.
  - **Использовать NTLM-аутентификацию с именем и паролем**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Security для Windows Server будет использовать указанную учетную запись для доступа к прокси-серверу. Введите имя и пароль пользователя или выберите пользователя в списке.



- **Применить имя и пароль пользователя**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.

7. В окне **Параметры программы** нажмите на кнопку **ОК**.

► *Чтобы настроить соединение с серверами обновлений "Лаборатории Касперского" в задаче обновления баз программы, выполните следующие действия:*

1. Запустите Консоль программы одним из следующих способов:

- Откройте Консоль программы на защищаемом устройстве. Для этого в меню **Пуск** выберите **Все программы > Kaspersky Security для Windows Server > Средства администрирования > Консоль Kaspersky Security для Windows Server**.
- Если Консоль программы запущена не на защищаемом устройстве, подключитесь к защищаемому устройству:
  - a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security для Windows Server**.
  - b. Выберите пункт **Подключиться к другому компьютеру**.
  - c. В окне **Выбор компьютера** выберите **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого устройства.

Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 281), укажите учетную запись, которая обладает этими правами.

Откроется окно Консоли программы.

2. В дереве Консоли программы разверните узел **Обновление**.
3. Выберите вложенный узел **Обновление баз программы**.
4. В панели результатов перейдите по ссылке **Свойства**.
5. В открывшемся окне **Параметры задачи** выберите закладку **Параметры соединения**.
6. Выберите **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.
7. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Параметры соединения с источником обновлений в задаче Обновление баз программы будут сохранены.

► *Чтобы запустить задачу Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз программы** выберите пункт **Запустить**.

Задача Обновление баз программы будет запущена.

После успешного завершения задачи можно посмотреть дату выпуска последних установленных обновлений баз программы в панели результатов узла **Kaspersky Security**.



## Проверка важных областей

После того как вы обновили базы Kaspersky Security для Windows Server, проверьте защищаемое устройство на наличие вредоносных программ с помощью задачи Проверка важных областей.

► Чтобы запустить задачу Проверка важных областей, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. В контекстном меню вложенного узла **Проверка важных областей** выберите команду **Запустить**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется**.

► Чтобы просмотреть журнал выполнения задачи,

в панели результатов узла **Проверка важных областей** перейдите по ссылке **Открыть журнал выполнения**.

## Изменение состава компонентов и восстановление Kaspersky Security для Windows Server

Вы можете добавлять или удалять компоненты Kaspersky Security для Windows Server. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу Постоянная защита файлов или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Security для Windows Server запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► Чтобы изменить состав компонентов Kaspersky Security для Windows Server, выполните следующие действия:

1. В меню **Пуск** выберите **Все программы > Kaspersky Security для Windows Server > Изменение или удаление**.

Откроется окно мастера установки программы **Изменение, восстановление или удаление установки**.

2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

3. В списке доступных компонентов в окне **Выборочная установка** выберите компоненты, которые требуется добавить или удалить из состава Kaspersky Security для Windows Server. Для этого выполните следующие действия:
  - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:
    - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;

- пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если требуется установить группу компонентов.
- Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

Нажмите на кнопку **Далее**.

4. В окне **Готовность к установке** подтвердите изменение состава компонентов программы, нажав на кнопку **Установить**.
5. В окне, открывшемся по завершении установки, нажмите на кнопку **ОК**.

Состав компонентов Kaspersky Security для Windows Server будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Security для Windows Server возникли проблемы (Kaspersky Security для Windows Server завершается аварийно, задачи завершаются аварийно или не запускаются), можно попробовать восстановить Kaspersky Security для Windows Server. Вы можете выполнить восстановление с сохранением текущих значений параметров Kaspersky Security для Windows Server или выбрать режим, при котором все параметры Kaspersky Security для Windows Server примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Security для Windows Server после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Security для Windows Server**.
3. Выберите **Изменение или удаление**.

Откроется окно мастера установки программы **Изменение, восстановление или удаление установки**.

4. Выберите вариант **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

Откроется окно **Восстановление установленных компонентов**.

5. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если вы хотите сбросить параметры программы и восстановить Kaspersky Security для Windows Server с параметрами по умолчанию. Нажмите на кнопку **Далее**.
6. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
7. В окне, открывшемся по завершении операции восстановления, нажмите на кнопку **ОК**.

Программа Kaspersky Security для Windows Server будет восстановлена с указанными параметрами.

## Удаление с помощью мастера установки

В этом разделе приведены инструкции по удалению Kaspersky Security для Windows Server, Консоли программы и расширения для Microsoft Outlook с защищаемого устройства с помощью мастера установки / удаления.

## В этом разделе

|                                                                    |                    |
|--------------------------------------------------------------------|--------------------|
| Удаление Kaspersky Security для Windows Server .....               | <a href="#">59</a> |
| Удаление Консоли Kaspersky Security для Windows Server .....       | <a href="#">60</a> |
| Удаление расширения Kaspersky Security для Microsoft Outlook ..... | <a href="#">60</a> |

## Удаление Kaspersky Security для Windows Server

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Security для Windows Server с защищаемого устройства с помощью мастера установки / удаления.

После удаления Kaspersky Security для Windows Server с защищаемого устройства может потребоваться перезагрузка. Перезагрузку можно отложить.

Удаление, восстановление и установка программы через панель управления Windows невозможна, если операционная система использует функцию Контроль учетных записей (User Account Control) или если доступ к управлению программой защищен паролем.

Если доступ к управлению программой защищен паролем, Kaspersky Security для Windows Server запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► Чтобы удалить Kaspersky Security для Windows Server, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Security для Windows Server**.
3. Выберите **Изменение или удаление**.  
Откроется окно мастера установки программы **Изменение, восстановление или удаление установки**.
4. Выберите пункт **Удаление компонентов программы**. Нажмите на кнопку **Далее**.  
Откроется окно **Дополнительные параметры удаления программы**.
5. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:
  - а. Установите флажок **Экспортировать объекты на карантин**, чтобы программа Kaspersky Security для Windows Server экспортировала объекты, помещенные на карантин. По умолчанию флажок снят.

- b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы экспортировать объекты из резервного хранилища Kaspersky Security для Windows Server. По умолчанию флажок снят.
- c. Нажмите на кнопку **Сохранить в** и укажите папку, в которую требуется экспортировать объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\Uninstall.

Нажмите на кнопку **Далее**.

6. В окне **Готовность к удалению** подтвердите удаление, нажав на кнопку **Удалить**.

7. В окне, открывшемся по завершении удаления, нажмите на кнопку **ОК**.

Программа Kaspersky Security для Windows Server будет удалена с защищаемого устройства.

## Удаление Консоли Kaspersky Security для Windows Server

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль программы с защищаемого устройства с помощью мастера установки / удаления.

После удаления Консоли программы перезагрузка защищаемого устройства не требуется.

► *Чтобы удалить Консоль программы, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Security для Windows Server**.
3. Выберите **Изменение или удаление Kaspersky Security для Windows Server**.  
Откроется окно мастера **Изменение или удаление**.
4. Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.
5. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.  
Откроется окно **Удаление завершено**.
6. Нажмите на кнопку **ОК**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

## Удаление расширения Kaspersky Security для Microsoft Outlook

► *Чтобы удалить расширение для Microsoft Outlook, выполните следующие действия:*

1. На защищаемом устройстве запустите файл setup.exe.  
Откроется окно приветствия мастера установки.
2. Нажмите на кнопку **Далее**.  
Откроется окно **Восстановление или удаление установки**.

3. Нажмите на кнопку **Удалить**.

Откроется окно **Готовность к удалению расширения Kaspersky Security для Microsoft Outlook**.

4. Нажмите на кнопку **Удалить**.

Мастер начнет установку расширения для Microsoft Outlook.

5. Нажмите на кнопку **Готово**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

## Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Security для Windows Server из командной строки, примеры команд для установки и удаления Kaspersky Security для Windows Server из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Security для Windows Server из командной строки.

### В этом разделе

|                                                                                         |                    |
|-----------------------------------------------------------------------------------------|--------------------|
| Об установке и удалении Kaspersky Security для Windows Server из командной строки ..... | <a href="#">61</a> |
| Примеры команд установки Kaspersky Security для Windows Server.....                     | <a href="#">62</a> |
| Действия после установки Kaspersky Security для Windows Server.....                     | <a href="#">64</a> |
| Добавление и удаление компонентов. Примеры команд.....                                  | <a href="#">65</a> |
| Удаление Kaspersky Security для Windows Server. Примеры команд.....                     | <a href="#">66</a> |
| Коды возврата .....                                                                     | <a href="#">67</a> |

## Об установке и удалении Kaspersky Security для Windows Server из командной строки

Для установки сертифицированной конфигурации Kaspersky Security для Windows Server необходимо включить установку компонентов Проверка скриптов, Kaspersky Endpoint Agent и Набор счетчиков производительности программы Системный монитор и выключить установку компонентов Контроль устройств, Управление сетевым экраном и Защита от сетевых угроз.

При установке сертифицированной конфигурации Kaspersky Security для Windows Server файл-маркер сертифицированной конфигурации должен находиться в одной папке с установщиком Kaspersky Security для Windows Server.

Защита сетевых хранилищ обеспечивается компонентами Защита RPC-подключаемых сетевых хранилищ, Защита ICAP-подключаемых сетевых хранилищ и Защита от шифрования для NetApp. Установите или снимите флажки напротив данных компонентов при установке сертифицированной конфигурации программы соответствующей типу вашей лицензии.

Вы можете устанавливать и удалять Kaspersky Security для Windows Server, добавлять или удалять его компоненты, запустив из командной строки файлы пакета установки `\server\ks4ws_x86.msi` или `\server\ks4ws_x64.msi` и указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом устройстве или на другом устройстве в сети, чтобы работать с Консолью программы локально или удаленно. Для этого используйте пакет установки `\client\ks4wstools.msi`.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на защищаемом устройстве, на котором установлена программа.

Если вы запустите на защищаемом устройстве один из файлов `\server\ks4ws_x86.msi` или `\server\ks4ws_x64.msi` без дополнительных ключей, программа Kaspersky Security для Windows Server будет установлена с рекомендуемыми параметрами установки.

Вы можете задать набор устанавливаемых компонентов с помощью ключа `ADDLOCAL`, перечислив в качестве его значений коды выбранных компонентов или наборов компонентов.

## Примеры команд установки Kaspersky Security для Windows Server

В этом разделе приведены примеры команд для установки Kaspersky Security для Windows Server.

На защищаемом устройстве под управлением 32-разрядной версии Microsoft Windows запускайте файлы с суффиксом `x86` из комплекта поставки. На защищаемом устройстве под управлением 64-разрядной версии Microsoft Windows запускайте файлы с суффиксом `x64` из комплекта поставки.

Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

### Примеры установки Kaspersky Security для Windows Server из файла `setup.exe`

- Чтобы установить Kaspersky Security для Windows Server с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:

```
\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

Kaspersky Security для Windows Server можно установить со следующими параметрами:

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать Постоянную защиту файлов при запуске Kaspersky Security для Windows Server;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

- Для этого выполните следующую команду:

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

- Чтобы установить Kaspersky Security для Windows Server с Kaspersky Endpoint Agent (см. стр. 27) без взаимодействия с пользователем, выполните следующую команду:

```
\server\setup.exe /s/p EULA=1 /p PRIVACYPOLICY=1 /p ADDLOCAL=Soyuz /p KEA_EULA=1
```

Можно использовать следующие дополнительные ключи команды:

```
/p "KEA_INSTALLDIR=\"<путь к папке установки>\""
```

Путь к пользовательской папке установки Kaspersky Endpoint Agent.

```
/p KEA_UNLOCK_PASSWORD=<пароль>
```

Задаёт защиту паролем, чтобы ограничить доступ пользователей к Kaspersky Endpoint Agent (для изменения, исправления, удаления).

```
/p KEA_PPL=<1|0>
```

Включает (1) или выключает (0) защиту процессов Kaspersky Endpoint Agent с помощью технологии AM-PPL (Antimalware Protected Process Light). Дополнительная информация о технологии AM-PPL приведена в Базе знаний Microsoft.

## Примеры команд для установки: запуск msi-файла

- Чтобы установить Kaspersky Security для Windows Server с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить Kaspersky Security для Windows Server с параметрами по умолчанию и показать интерфейс установки, выполните следующую команду:

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить Kaspersky Security для Windows Server и активировать с помощью файла ключа C:\0000000A.key, выполните следующую команду:

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1  
PRIVACYPOLICY=1
```

- Чтобы установить Kaspersky Security для Windows Server с предварительной проверкой активных процессов и загрузочных секторов локальных дисков, выполните следующую команду:

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить Kaspersky Security для Windows Server в папку установки C:\WSEE, выполните следующую команду:

```
msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1
```



- Чтобы установить Kaspersky Security для Windows Server и сохранить файл журнала установки с именем *ks4ws.log* в папку, где хранится *msi*-файл Kaspersky Security для Windows Server, выполните следующую команду:

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить Консоль Kaspersky Security для Windows Server, выполните следующую команду:

```
msiexec /i ks4wstools.msi /qn EULA=1
```

- Чтобы установить расширение для Microsoft Outlook для 64-разрядного почтового клиента Microsoft Outlook, выполните следующую команду

```
msiexec /i ksmail_x64.msi /qn EULA=1
```

- Чтобы установить расширение для Microsoft Outlook для 32-разрядного почтового клиента Microsoft Outlook, выполните следующую команду

```
msiexec /i ksmail_x86.msi /qn EULA=1
```

- Чтобы установить Kaspersky Security для Windows Server и активировать программу с помощью файла ключа *C:\0000000A.key*, а также настроить Kaspersky Security для Windows Server в соответствии с параметрами в конфигурационном файле *C:\settings.xml*, выполните следующую команду:

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key  
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить исправление, если программа Kaspersky Security для Windows Server защищена паролем, выполните следующую команду:

```
msiexec /p "<msp путь к имени файла>" UNLOCK_PASSWORD=<пароль>
```

## Действия после установки Kaspersky Security для Windows Server

Kaspersky Security для Windows Server запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Security для Windows Server был установлен флажок **Включить постоянную защиту после установки программы**, программа проверяет объекты файловой системы устройства при доступе к ним. Если при выборочной установке был установлен компонент Проверка скриптов, Kaspersky Security для Windows Server будет выполнять проверку программного кода для всех скриптов при их запуске. Каждую пятницу в 20:00 Kaspersky Security для Windows Server выполняет задачу Проверка важных областей.

После установки Kaspersky Security для Windows Server рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Security для Windows Server. После установки Kaspersky Security для Windows Server проверяет объекты с использованием баз, которые входили в состав программы при поставке. Рекомендуется сразу же обновить базы Kaspersky Security для Windows Server. Для этого вам нужно запустить задачу Обновление баз программы. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию.



Например, вы можете запустить задачу Обновление баз программы, выполнив следующую команду:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
```

При этом обновления баз Kaspersky Security для Windows Server будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080) с использованием для доступа к серверу встроенной в Windows проверки подлинности NTLM с учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить Проверку важных областей, если перед установкой Kaspersky Security для Windows Server на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Чтобы выполнить задачу Проверка важных областей с помощью командной строки, выполните следующую команду:

```
KAVSHELL SCANCritical W:scancritical.log
```

Эта команда сохраняет журнал выполнения задачи в файле scancritical.log в текущей папке.

- Настроить уведомления администратора о событиях Kaspersky Security для Windows Server.

## Добавление и удаление компонентов. Примеры команд

Компонент Проверка по требованию устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Security для Windows Server.

- Чтобы добавить компонент Контроль запуска программ к ранее установленным компонентам, выполните следующую команду:

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn
```

или

```
\server\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Если вы перечислите не только компоненты, которые требуется установить, но и уже установленные компоненты, Kaspersky Security для Windows Server переустановит указанные установленные компоненты.

- Чтобы удалить установленные компоненты, выполните следующую команду:

```
msiexec /i ks4ws.msi  
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram Disk REMOVE=AppCtrl,Fim" /qn
```

## Удаление Kaspersky Security для Windows Server. Примеры команд

- Чтобы удалить Kaspersky Security для Windows Server с защищаемого устройства, выполните следующую команду:

```
msiexec /x ks4ws.msi /qn
```

или

- Для 32-разрядной операционной системы:

```
msiexec /x {6607EF9A-4D10-4D3E-B255-6F280BFB3791} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843} /qn
```

- Чтобы удалить Консоль Kaspersky Security для Windows Server, выполните следующую команду:

```
msiexec /x ks4wstools.msi /qn
```

или

- Для 32-разрядной операционной системы:

```
msiexec /x {54B7D218-5645-46DD-8660-41B336E1BD8A} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {C10F9B07-7FC9-43C0-A5DC-B6CE8A817D76} /qn
```

- Чтобы удалить Kaspersky Security для Windows Server с защищаемого устройства, на котором установлена защита паролем, выполните следующую команду:

- Для 32-разрядной операционной системы:

```
msiexec /x {6607EF9A-4D10-4D3E-B255-6F280BFB3791} UNLOCK_PASSWORD=*** /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843} UNLOCK_PASSWORD=*** /qn
```

- Чтобы удалить расширение для Microsoft Outlook, выполните следующую команду:

- Для 32-разрядной операционной системы:

```
msiexec /x {6AF88E70-817E-4FFE-8389-04A345E7A3D6} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {410BC997-5B96-41B3-8B31-AAA074FE728B} /qn
```

## Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

Table 4. Коды возврата

| Код   | Описание                                                                                                                                                                                                                              |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1324  | Имя папки назначения содержит недопустимые символы.                                                                                                                                                                                   |
| 25001 | Недостаточно прав для установки Kaspersky Security для Windows Server. Чтобы установить программу, запустите мастер установки с правами локального администратора.                                                                    |
| 25003 | Не удается установить Kaspersky Security для Windows Server на устройство под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows. |
| 25004 | Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующее программное обеспечение: <список несовместимого программного обеспечения>.                                                            |
| 25010 | Указанный путь не может быть использован для сохранения объектов на карантине.                                                                                                                                                        |
| 25011 | Имя папки для сохранения объектов на карантине содержит недопустимые символы.                                                                                                                                                         |
| 26251 | Не удалось загрузить DLL для Счетчиков производительности.                                                                                                                                                                            |
| 26252 | Не удалось загрузить DLL для Счетчиков производительности.                                                                                                                                                                            |
| 27300 | Драйвер не может быть установлен.                                                                                                                                                                                                     |
| 27301 | Драйвер не может быть удален.                                                                                                                                                                                                         |
| 27302 | Невозможно установить сетевой компонент. Достигнуто максимальное пороговое значение поддерживаемого количества устройств фильтрации.                                                                                                  |
| 27303 | Антивирусные базы не найдены.                                                                                                                                                                                                         |

## Установка и удаление программы с помощью Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Security для Windows Server через Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Security для Windows Server через Kaspersky Security Center, а также описание действий после установки Kaspersky Security для Windows Server.

### В этом разделе

|                                                                                       |                    |
|---------------------------------------------------------------------------------------|--------------------|
| Общие сведения об установке через Kaspersky Security Center .....                     | <a href="#">68</a> |
| Права для установки и удаления Kaspersky Security для Windows Server .....            | <a href="#">68</a> |
| Установка Kaspersky Security для Windows Server через Kaspersky Security Center ..... | <a href="#">69</a> |
| Действия после установки Kaspersky Security для Windows Server .....                  | <a href="#">71</a> |
| Установка Консоли программы через Kaspersky Security Center .....                     | <a href="#">72</a> |
| Удаление Kaspersky Security для Windows Server через Kaspersky Security Center .....  | <a href="#">73</a> |

## Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Security для Windows Server через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки программа Kaspersky Security для Windows Server будет установлена с одинаковыми параметрами на несколько защищаемых устройств.

Можно объединить все защищаемые устройства в одну группу администрирования и создать групповую задачу установки Kaspersky Security для Windows Server на защищаемые устройства этой группы.

Вы можете создать задачу удаленной установки Kaspersky Security для Windows Server для набора защищаемых устройств, не объединенных в одну группу администрирования. При создании этой задачи нужно сформировать список отдельных защищаемых устройств, на которые требуется установить Kaspersky Security для Windows Server.

Подробная информация о задаче удаленной установки приведена в *Справке Kaspersky Security Center*.

## Права для установки или удаления Kaspersky Security для Windows Server

Учетная запись, указанная в задаче удаленной установки (удаления), должна входить в группу администраторов на каждом защищаемом устройстве во всех случаях, кроме следующих ситуаций:

- На защищаемых устройствах, на которых требуется установить Kaspersky Security для Windows Server, уже установлен Агент администрирования Kaspersky Security Center (независимо от того, в каком домене находятся защищаемые устройства и принадлежат ли они к какому-либо домену).

Если Агент администрирования еще не установлен на защищаемых устройствах, вы можете установить его вместе с Kaspersky Security для Windows Server с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом защищаемом устройстве.

- Все защищаемые устройства, на которые вы хотите установить Kaspersky Security для Windows Server, находятся в одном домене с Сервером администрирования и Сервер администрирования зарегистрирован под учетной записью **Администратор домена** (Domain Admin), если эта учетная запись обладает правами локального администратора на защищаемых устройствах домена.

По умолчанию задача удаленной установки методом **Форсированная установка** запускается с правами той учетной записи, под которой работает Сервер администрирования.

В групповых задачах и в задачах для набора защищаемых устройств, в которых был выбран метод форсированной установки (удаления), учетная запись должна обладать следующими правами на защищаемом устройстве:

- правом на удаленный запуск программ;
- доступом к папке общего доступа **Admin\$**;
- правом **Вход в качестве службы**.

## Установка Kaspersky Security для Windows Server через Kaspersky Security Center

Подробная информация о формировании инсталляционного пакета о и создании задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

Если вы планируете в дальнейшем управлять Kaspersky Security для Windows Server через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На защищаемом устройстве с установленным Сервером администрирования Kaspersky Security Center также установлен Плагин управления (файл \server\klcfginst.exe комплекта поставки Kaspersky Security для Windows Server).
- На защищаемых устройствах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых устройствах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Security для Windows Server в задаче удаленной установки.

Можно также объединить устройства в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

► Чтобы установить Kaspersky Security для Windows Server с помощью задачи удаленной установки, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Дополнительно**.

3. Разверните вложенный узел **Удаленная установка**.
4. В рабочей области узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.
5. Выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. Введите имя инсталляционного пакета.
7. Выберите файл ks4ws.kud из комплекта поставки Kaspersky Security для Windows Server в качестве файла инсталляционного пакета.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

8. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения и Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности**.

Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.

9. Чтобы изменить набор устанавливаемых компонентов Kaspersky Security для Windows Server (см. раздел "Изменение состава компонентов и восстановление Kaspersky Security для Windows Server" на стр. 57) и параметры установки по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows " на стр. 38) в инсталляционном пакете, выполните следующие действия:
  - a. В Kaspersky Security Center разверните узел **Удаленная установка**.
  - b. В панели результатов вложенного узла **Инсталляционные пакеты** откройте контекстное меню созданного инсталляционного пакета Kaspersky Security для Windows Server и выберите пункт **Свойства**.
  - c. В окне **Свойства: <название инсталляционного пакета>** перейдите раздел **Настройка**.
  - d. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Security для Windows Server, которые вы хотите установить.
  - e. Чтобы установить Kaspersky Endpoint Agent (см. стр. 27), выполните следующие действия:
    1. Нажмите на кнопку **Лицензионное соглашение**.  
Откроется окно **Условия Положения о Kaspersky Endpoint Agent**.
    2. Ознакомьтесь с условиями Положения о Kaspersky Endpoint Agent.
    3. Установите флажок **Я принимаю условия Положения о Kaspersky Endpoint Agent**.
    4. Нажмите на кнопку **ОК**.
    5. Установите флажок **Установить Kaspersky Endpoint Agent**.

Флажок **Установить Kaspersky Endpoint Agent** недоступен, если не был установлен флажок **Я принимаю условия Положения о Kaspersky Endpoint Agent**.

- f. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.
- Путь к папке назначения может содержать системные переменные окружения. Если указанной папки не существует на защищаемом устройстве, она будет создана.
- g. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:
- **Выполнить антивирусную проверку сервера перед началом установки**
  - **Включить постоянную защиту после установки программы**
  - **Добавить к исключениям файлы, рекомендованные Microsoft**
  - **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**
- h. Если вы хотите импортировать параметры из конфигурационного файла, созданного в предыдущей версии Kaspersky Security для Windows Server, укажите конфигурационный файл.
- i. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.
10. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Security для Windows Server на защищаемые устройства (группу администрирования). Настройте параметры задачи.
- Подробная информация о создании и настройке задачи удаленной установки содержится в *Справке Kaspersky Security Center*.
11. Запустите задачу удаленной установки Kaspersky Security для Windows Server.
- Программа Kaspersky Security для Windows Server будет установлена на указанные в задаче защищаемые устройства.

## Действия после установки Kaspersky Security для Windows Server

После установки Kaspersky Security для Windows Server рекомендуется обновить базы Kaspersky Security для Windows Server на устройствах, а также выполнить Проверку важных областей устройств, если до установки Kaspersky Security для Windows Server на устройствах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если защищаемые устройства, на которых установлена программа Kaspersky Security для Windows Server, объединены в одну группу администрирования в Kaspersky Security Center, можно выполнить эти задачи следующими способами:

1. Создать задачу обновления баз программы для группы защищаемых устройств, на которых установлена программа Kaspersky Security для Windows Server. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
2. Создать групповую задачу проверки по требованию со статусом Проверка важных областей. Kaspersky Security Center оценивает состояние безопасности каждого защищаемого устройства группы по результатам выполнения этой задачи, а не по результатам задачи Проверка важных областей.
3. Создать новую политику для группы защищаемых устройств. В свойствах политики в разделе **Параметры программы** выключить запуск по расписанию системных задач проверки по требованию и задачи Обновление баз программы на защищаемых устройствах группы администрирования в подразделе **Запуск системных задач**.

Можно также настроить уведомления администратора о событиях Kaspersky Security для Windows Server.

## Установка Консоли программы через Kaspersky Security Center

Подробная информация о создании инсталляционного пакета и задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

► Чтобы установить Консоль программы с помощью задачи удаленной установки, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.
2. Разверните вложенный узел **Удаленная установка**.
3. В рабочей области узла Инсталляционные пакеты нажмите на кнопку **Создать инсталляционный пакет**. При создании нового инсталляционного пакета:
  - a. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет для указанного исполняемого файла** в качестве типа пакета.
  - b. Введите имя инсталляционного пакета.
  - c. В папке комплекта поставки Kaspersky Security для Windows Server выберите файл client\setup.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.
  - d. Если требуется, с помощью ключа командной строки ADDLOCAL измените состав устанавливаемых компонентов в поле **Параметры запуска исполняемого файла (необязательно)** и папку назначения.

Например, чтобы установить только Консоль программы в папку C:\KasperskyConsole, не устанавливая файлы справки и документации, используйте следующие ключи командной строки:

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
```

4. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли программы на выбранные защищаемые устройства (группу администрирования). Настройте параметры задачи.

Подробная информация о создании и настройке задач удаленной установки содержится в Справке Kaspersky Security Center.

5. Запустите задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче защищаемые устройства.



## Удаление Kaspersky Security для Windows Server через Kaspersky Security Center

Если доступ к управлению Kaspersky Security для Windows Server на устройствах сети защищен паролем, введите пароль при создании задачи удаления нескольких программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, программа Kaspersky Security для Windows Server будет успешно удалена с устройств, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Программа Kaspersky Security для Windows Server не будет удалена с других защищаемых устройств.

► Чтобы удалить Kaspersky Security для Windows Server, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программы.
2. В задаче выберите метод удаления (аналогично выбору метода установки, см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к защищаемым устройствам. Вы можете удалить Kaspersky Security для Windows Server только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. [38](#)).

## Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Security для Windows Server через групповые политики Active Directory, а также информацию о действиях, которые требуется выполнить после установки Kaspersky Security для Windows Server через групповые политики.

### В этом разделе

|                                                                                                 |                    |
|-------------------------------------------------------------------------------------------------|--------------------|
| Установка Kaspersky Security для Windows Server через групповые политики Active Directory ..... | <a href="#">73</a> |
| Действия после установки Kaspersky Security для Windows Server .....                            | <a href="#">74</a> |
| Удаление Kaspersky Security для Windows Server через групповые политики Active Directory .....  | <a href="#">75</a> |

## Установка Kaspersky Security для Windows Server через групповые политики Active Directory

Вы можете установить Kaspersky Security для Windows Server на несколько защищаемых устройств с помощью групповой политики Active Directory. Консоль программы можно установить аналогичным образом.

Защищаемые устройства, на которые требуется установить Kaspersky Security для Windows Server или Консоль программы, должны быть в одном домене и в одной организационной единице.

Операционные системы защищаемых устройств, на которые требуется установить Kaspersky Security для Windows Server с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Security для Windows Server, используйте пакет установки ks4ws\_x86.msi или ks4ws\_x64.msi. Чтобы установить Консоль программы, используйте пакет установки ks4wstools.msi.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

► Чтобы установить Kaspersky Security для Windows Server (или Консоль программы), выполните следующие действия:

1. Сохраните msi-файл, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папку общего доступа на контроллере домена.
2. Сохраните файл ключа (см. раздел "О файле ключа" на стр. [Ошибка! Закладка не определена.](#)) в эту же общую папку на контроллере домена.
3. В этой же папке общего доступа на контроллере домена создайте файл install\_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

```
{  
  "EULA": "1",  
  "PRIVACYPOLICY": "1"  
}
```

4. На контроллере домена создайте новую политику для группы, в которую объединены защищаемые устройства.
5. С помощью **Редактора объектов групповых политик** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу Kaspersky Security для Windows Server или Консоли программы в формате UNC (Universal Naming Convention).
6. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
7. Примените изменения с помощью команды `gpupdate / force`.

Программа Kaspersky Security для Windows Server будет установлена на защищаемые устройства группы после их перезагрузки.

## Действия после установки Kaspersky Security для Windows Server

После установки Kaspersky Security для Windows Server на защищаемые устройства рекомендуется сразу обновить базы программы и выполнить Проверку важных областей. Вы можете выполнить эти действия из Консоли программы (см. раздел "Действия после установки Kaspersky Security для Windows Server" на стр. [54](#)).

Можно также настроить уведомления администратора о событиях Kaspersky Security для Windows Server.

## Удаление Kaspersky Security для Windows Server через групповые политики Active Directory

Если вы установили Kaspersky Security для Windows Server или Консоль программы в группе управляемых устройств, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Security для Windows Server или Консоль программы.

Вы можете удалить программу только с параметрами удаления по умолчанию.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Если доступ к управлению программой защищен паролем, удаление Kaspersky Security для Windows Server через групповые политики Active Directory невозможно.

► Чтобы удалить Kaspersky Security для Windows Server (или Консоль программы), выполните следующие действия:

1. На контроллере домена выберите организационную единицу, с защищаемых устройств которой требуется удалить Kaspersky Security для Windows Server или Консоль программы.
2. Выберите политику, созданную для установки Kaspersky Security для Windows Server, и в **Редакторе объектов групповых политик**, в узле **Установка программ (Конфигурация компьютеров > Параметры программ > Установка программ)** откройте контекстное меню пакета установки Kaspersky Security для Windows Server (Консоли программы) и выберите команду **Все задачи > Удалить**.
3. Выберите метод удаления **Немедленно удалить программы из учетных записей пользователей и компьютеров**.
4. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Security для Windows Server будет удален с защищаемых устройств после их перезагрузки, перед входом в Microsoft Windows.

# Проверка функций Kaspersky Security для Windows Server. Использование тестового вируса EICAR

В этом разделе описан тестовый вирус EICAR и его использование для проверки функций постоянной защиты файлов и проверки по требованию Kaspersky Security для Windows Server.

## В этом разделе

|                                                                          |                    |
|--------------------------------------------------------------------------|--------------------|
| О тестовом вирусе EICAR .....                                            | <a href="#">76</a> |
| Проверка функций постоянной защиты файлов и проверки по требованию ..... | <a href="#">77</a> |

## О тестовом вирусе EICAR

Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вредоносным объектом и не содержит исполняемого кода, который может нанести вред вашему устройству, но антивирусные программы большинства производителей идентифицируют его как угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Его можно загрузить на веб-сайте EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Перед сохранением файла в папку на жестком диске устройства убедитесь, что Постоянная защита файлов выключена для этого жесткого диска.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Security для Windows Server обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы и в журнале выполнения задачи.

Вы также можете использовать файл eicar.com, чтобы проверять, как Kaspersky Security для Windows Server выполняет лечение зараженных объектов и обнаруживает возможно зараженные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из префиксов, перечисленных в таблице ниже, и сохраните файл с новым именем, например, eicar\_cure.com.

Чтобы убедиться, что Kaspersky Security для Windows Server обрабатывает файл eicar.com с префиксом, в разделе параметров безопасности **Защита объектов** установите значение **Все объекты** для задач постоянной защиты сервера и проверки по требованию в Kaspersky Security для Windows Server.

Table 5. Префиксы в файлах EICAR

| Префикс      | Статус файла после проверки и действие Kaspersky Security для Windows Server                                                                                                                                                             |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Без префикса | Kaspersky Security для Windows Server присваивает объекту статус <b>Зараженный</b> и удаляет его.                                                                                                                                        |
| SUSP–        | Kaspersky Security для Windows Server присваивает статус <b>Возможно зараженный</b> объекту, обнаруженному с помощью эвристического анализатора, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.           |
| WARN–        | Kaspersky Security для Windows Server присваивает статус <b>Возможно зараженный</b> объекту, если код объекта частично совпадает с кодом известной угрозы, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению. |
| CURE–        | Kaspersky Security для Windows Server присваивает объекту статус <b>Зараженный</b> и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".                                                                       |

## Проверка функций постоянной защиты файлов и проверки по требованию

После установки Kaspersky Security для Windows Server вы можете убедиться, что Kaspersky Security для Windows Server обнаруживает объекты, содержащие вредоносный код. Для этого можно использовать тестовый вирус EICAR (см. раздел "О тестовом вирусе EICAR" на стр. 76).

► Чтобы проверить функцию постоянной защиты файлов, выполните следующие действия:

1. Загрузите файл eicar.com с веб-сайта EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Сохраните его в папку общего доступа на локальном диске любого устройства сети.

Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что Служба сообщений Microsoft Windows включена на защищаемом устройстве и на устройстве, на котором сохранен файл eicar.com.
3. Откройте Консоль программы на защищаемом устройстве.
4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого устройства одним из следующих способов:
  - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на защищаемое устройство, подключившись к защищаемому устройству с помощью программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).
  - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с устройства, на котором вы его сохранили, через сетевое окружение этого устройства.

Постоянная защита файлов работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с защищаемого устройства.

- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Постоянная защита сервера**, выберите задачу **Постоянная защита файлов** и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.
- На устройстве, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: Программа Kaspersky Security для Windows Server заблокировала доступ к <путь к файлу eicar.com на устройстве>\eicar.com на компьютере <сетевое имя устройства> в <время возникновения события>. Причина: обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <имя пользователя>. Имя компьютера: <сетевое имя устройства, с которого вы скопировали файл>.

Убедитесь, что Служба сообщений Microsoft Windows работает на устройстве, с которого вы скопировали файл eicar.com.

► Чтобы проверить функцию проверки по требованию, выполните следующие действия:

1. Загрузите файл eicar.com с веб-сайта EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Сохраните его в папку общего доступа на локальном диске любого устройства сети.

Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Откройте Консоль программы (см. раздел "Запуск Консоли Kaspersky Security для Windows Server из меню Пуск" на стр. 272).
3. Выполните следующие действия:
  - a. В дереве Консоли программы разверните узел **Проверка по требованию**.
  - b. Выберите вложенный узел **Проверка важных областей**.
  - c. На закладке **Параметры области проверки** откройте контекстное меню узла **Сетевое окружение** и выберите пункт **Добавить сетевой файл**.
  - d. Введите сетевой путь к файлу eicar.com на удаленном устройстве в формате UNC (Universal Naming Convention).
  - e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.
  - f. Запустите задачу Проверка важных областей.

Проверка по требованию работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с жесткого диска устройства.
- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале выполнения задачи проверки важных областей появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Проверка по требованию**, выберите задачу Проверка важных областей и в панели результатов перейдите по ссылке **Открыть журнал выполнения**.

# Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

## В этом разделе

|                                         |                    |
|-----------------------------------------|--------------------|
| Безопасное состояние .....              | <a href="#">76</a> |
| Проверка работоспособности. EICAR ..... | <a href="#">77</a> |

## Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу.

Вы можете производить настройку параметров для всех защищаемых компьютеров с помощью политики в Kaspersky Security Center или для одного компьютера с помощью локальной Консоли администратора, установленной на этом компьютере.

## Настройка прав доступа

По умолчанию доступ ко всем функциям Kaspersky Security для Windows Server, управлению службами Kaspersky Security Service (KAVFS) и Kaspersky Security Management Service (KAVFSGT) имеют пользователи, входящие в группу «Администраторы» на защищаемом компьютере, пользователи группы «KWS Administrators», созданной на защищаемом компьютере при установке Kaspersky Security для Windows Server, а также системная группа «SYSTEM».

Пользователи-администраторы, осуществляющие контроль за безопасностью должны быть добавлены в группу «KWS Administrators» с правами полного доступа к управлению службами и функциями программы.

► Чтобы добавить пользователя, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите пункт **Изменить права пользователей на управление программой**.  
Откроется окно **Разрешения для группы «Kaspersky Security для Windows Server»**.
3. В открывшемся окне в списке **Группы или пользователи** выберите группу «KWS Administrators» и нажмите кнопку **Добавить**.

4. В открывшемся окне введите название учетной записи, которую необходимо добавить.
5. В блоке **Разрешения для группы «KSWs Administrators»** убедитесь, что установлены флажки **Разрешить для следующих пунктов**:
  - **Полный контроль**: полный набор прав на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service.
  - **Чтение**:
    - следующие права на управление Kaspersky Security для Windows Server: **Чтение статистики, Чтение параметров, Чтение журналов и Чтение прав**;
    - следующие права на управление службой Kaspersky Security Service: **Чтение параметров службы, Запрос статуса службы у Диспетчера управления службами, Запрос статуса у службы, Перечисление зависимых служб, Чтение прав**.
  - **Изменение**:
    - все права на управление Kaspersky Security для Windows Server, кроме **Изменение прав**;
    - следующие права на управление службой Kaspersky Security Service: **Изменение параметров службы, Чтение прав**.
  - **Исполнение**: следующие права на управление службой Kaspersky Security Service: **Запуск службы, Остановка службы, Приостановка / Возобновление службы, Чтение прав, Пользовательские запросы к службе**.
6. В окне **Разрешения для группы «Kaspersky Security для Windows Server»** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service будут сохранены.

Для настройки доступа к службам Kaspersky Security для Windows Server, в контекстном меню узла **Kaspersky Security для Windows Server** выберите пункт **Изменить права пользователей на управление Kaspersky Security Service** и выполните шаги 3-6.

Для всех пользователей и групп, кроме «KSWs Administrators» и «SYSTEM», установите флажки **Запретить** для всех пунктов.



## Сигналы тревоги

► Чтобы настроить уведомления о событиях при обнаружении тревоги, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

Откроется окно **Параметры журналов**.

2. На закладке **Уведомления** в блоке **Уведомление администраторов** установите флажок **Путем запуска исполняемого файла** для следующих типов событий:

- Обнаружен объект.
- Объект не вылечен.
- Объект не удален.
- Объект не помещен на карантин.
- Объект не помещен в резервное хранилище.
- Запуск программы запрещен.
- Запуск программы запрещен по прецеденту.

3. Нажмите на кнопку **Настройка**.

Откроется окно **Дополнительные параметры**.

4. Выберите закладку **Исполняемый файл** и выполните следующие действия:

- a. В поле **Командная строка** укажите исполняемый файл, который программа будет запускать при обнаружении событий нарушения безопасности.  
Запускаемая программа должна обеспечивать непрерывную выдачу сигнала нарушения безопасности.
- b. В блоке **Запуск с правами** укажите данные учетной записи Администратора.
- c. Нажмите на кнопку **ОК**.

5. На закладке **Уведомления** нажмите на кнопку **Текст сообщения**.

6. В открывшемся окне укажите информацию, которую Kaspersky Security для Windows Server будет передавать в составе сигнала тревоги.

Убедитесь, что в тексте сообщения присутствуют следующие переменные: **Тип обнаруженного объекта** (%VIRUS\_TYPE%), **Обнаружено** (%VIRUS\_NAME%) и **Событие** (%EVENT\_TYPE%). Если данные переменные отсутствуют, добавьте их с помощью раскрывающегося списка по кнопке **Макрос**. Удаление перечисленных переменных приводит к выходу программы из сертифицируемого состояния.

7. Нажмите на кнопку **ОК**.

Настройки уведомлений администраторов будут сохранены.

Сообщение сигнала тревоги не содержит данных о действиях по обработке. Kaspersky Security для Windows Server сообщает о неудачном результате обработки посредством отдельного сигнала тревоги. Отсутствие сигнала тревоги о неудачной обработке события означает, что объект был обработан в соответствии с настроенными параметрами защиты и проверки.

При неудачном результате обработки Kaspersky Security для Windows Server отображает одно из следующих событий:

- Срок действия лицензии истек.
- Базы программы сильно устарели.
- Внутренняя ошибка.
- Внутренняя ошибка программы.
- Базы программы устарели.
- Срок действия лицензии скоро истечет.

## Блокирование сервера с установленным Kaspersky Security для Windows Server при обнаружении зараженных объектов

Kaspersky Security для Windows Server поддерживает запуск сторонних программ, которые позволяют отключить скомпрометированный сервер, на котором обнаружен зараженный объект, от локальной сети. Блокирование сервера осуществляется с помощью настройки уведомлений о событиях, которые будут являться триггерами для запуска сторонней программы.

Чтобы настроить запуск программы для блокировки скомпрометированного сервера, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Журналы и уведомления**.
2. Откройте контекстное меню и выберите пункт **Свойства**.
3. Откроется окно **Параметры журналов и уведомлений**.
4. Выберите закладку **Уведомления**.
5. В списке типов событий выберите событие **Обнаружен объект**.
6. В блоке **Уведомления администраторов** настройте параметры запуска сторонней программы:

a. Установите флажок **Путем запуска исполняемого файла**.

b. Нажмите на кнопку **Настройка**.

Откроется окно **Дополнительные параметры**.

c. Перейдите на закладку **Исполняемый файл**.

d. В поле **Командная строка** введите имя исполняемого файла или нажмите кнопку **Обзор** для выбора файла через проводник Windows.

e. В окне **Дополнительные параметры** нажмите на кнопку **ОК**.

7. В окне **Параметры журналов и уведомлений** нажмите на кнопку **ОК**.

## События аудита

Kaspersky Security для Windows Server ведет системный аудит событий, связанных с управлением Kaspersky Security для Windows Server. Для функционирования в сертифицированном состоянии программа должна фиксировать все события для компонентов Постоянная защита, Проверка по требованию, Контроль запуска программ.

► Чтобы настроить события аудита для данных компонентов выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

Откроется окно **Параметры Журналов**.

2. На закладке **Общие**, установите флажок **Все события** для следующих компонентов:

- Постоянная защита файлов;
- Проверка по требованию;
- Контроль запуска программ.

3. Нажмите на кнопку **ОК**.

## Постоянная защита файлов

Для приведения программы в сертифицируемое состояние, требуется произвести донастройку параметров задачи. По умолчанию задача Постоянная защита файлов не выполняет проверку архивов.

► Чтобы добавить архивы к проверяемым объектам, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

Откроется окно **Настройка области защиты**.

4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.
5. На закладке **Общие** в блоке **Защита составных объектов** установите флажок **Все / Только новые архивы**.

Параметр **Только новые архивы** доступен, если снят флажок **Проверка только новых и измененных файлов**.

6. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server будет выполнять проверку архивов ZIP, CAB, RAR, ARJ и других форматов.

## Проверка по требованию

В соответствии с требованиями сертификации, необходимо создать новую пользовательскую задачу Проверки по требованию и запустить ее с предзаданными параметрами.

Подробная инструкция по созданию задач проверки по требованию содержится в разделе «Задача Проверка по требованию».

## Настройка обновлений баз программы

► Чтобы настроить обновление антивирусных баз через один из защищаемых компьютеров, который выполняет функцию компьютера-ретранслятора, выполните следующие действия:

1. На компьютере-ретрансляторе остановите выполнение задач Обновление баз программы и Обновление модулей программы.
2. Настройте параметры задачи Копирование обновлений:
  - На закладке **Общие**:

- В блоке **Источник обновлений** выберите **Серверы обновлений «Лаборатории Касперского»**.
  - В блоке **Параметры копирования обновлений** выберите **Копировать обновления баз программы**.
  - В поле **Папка локального источника обновлений** укажите путь к общей сетевой папке, в которую программа будет сохранять скопированный файл баз. Программа не распаковывает и не применяет обновления, загруженные с помощью задачи копирования баз.
  - На закладке **Параметры соединения** установите флажок **Использовать параметры прокси-сервера для соединения с серверами «Лаборатории Касперского»**.
  - На закладке **Расписание** установите флажок **Запускать задачу по расписанию** с частотой запуска **Ежечасно**.
3. На компьютере-ретрансляторе запустите задачу Копирование обновлений.
4. На компьютерах-ресиверах настройте параметры задачи Обновление баз программы, выполнив следующие действия:
- a. На закладке **Общие** укажите в качестве источника обновлений **Другие HTTP-, FTP-серверы или сетевые ресурсы**. В качестве источника укажите сетевую папку, настроенную в качестве папки локального источника обновлений в задаче Копирование обновлений на сервере-ретрансляторе.
  - b. Снимите флажок **Использовать серверы обновлений «Лаборатории Касперского»**, если серверы, указанные пользователем, недоступны.
  - c. Настройте расписание запуска задачи Обновление баз программы на компьютерах-ресиверах таким образом, чтобы:
    - Задача выполнялась ежечасно.
    - Запуск задачи выполнялся с шагом 30 минут после запуска задачи Копирование обновлений на сервере-ретрансляторе.

Обновления баз программы, загруженные из локальной папки обновлений на компьютеры-ресиверы, будут немедленно применены и распакованы.

## Установка расширения для защиты от почтовых угроз

Защита от почтовых угроз предоставляется через расширение для Microsoft Outlook и устанавливается отдельно от компонентов Kaspersky Security для Windows Server.

Вы можете установить расширение для Microsoft Outlook только если на защищаемом сервере установлены Kaspersky Security для Windows Server и почтовый клиент Microsoft Outlook.

- Чтобы установить расширение, запустите пакет *ksmail\_x86(x64).msi* из папки *lemail\_plugin*.

## Настройка путей для распаковки проверяемых архивов в системном реестре

Антивирусная проверка ICAP-подключаемых сетевых хранилищ позволяет выявлять потенциально опасные файлы в архивах. Вы можете настроить путь, куда будут распаковываться файлы из всех проверяемых архивов на сервере.

Чтобы настроить путь в редакторе реестра операционной системы:

4. Перейдите по пути:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment].
5. Введите путь к папке в виде: "ProcessingTempPath"="d:\\Temp\\".

## Проверка работоспособности. EICAR

Чтобы проверить работоспособность Антивируса, вы можете использовать тестовый "вирус" EICAR.

Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Файл, который содержит тестовый вирус, называется *eicar.com*. Его можно загрузить на веб-сайте EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Security для Windows Server обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы, в журнале выполнении задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Kaspersky Security для Windows Server выполняет лечение зараженных объектов и как он обнаруживает возможно зараженные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из префиксов, перечисленных в таблице ниже, и сохраните файл под новым именем, например, eicar\_cure.com.

Для того чтобы Kaspersky Security для Windows Server обработал файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задач Kaspersky Security для Windows Server Постоянная защита файлов и задач проверки по требованию.

Table 6. Префиксы в файлах EICAR

| Префикс      | Статус файла после проверки и действие Kaspersky Security для Windows Server                                                                                                                                                    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Без префикса | Kaspersky Security для Windows Server присваивает объекту статус <b>Зараженный</b> и удаляет его.                                                                                                                               |
| SUSP–        | Kaspersky Security для Windows Server присваивает объекту статус <b>Возможно зараженный</b> (обнаружен с помощью эвристического анализатора) и удаляет его (возможно зараженные объекты не подвергаются лечению).               |
| WARN–        | Kaspersky Security для Windows Server присваивает объекту статус <b>Возможно зараженный</b> (код объекта частично совпадает с известным вредоносным кодом) и удаляет его (возможно зараженные объекты не подвергаются лечению). |
| CURE–        | Kaspersky Security для Windows Server присваивает объекту статус <b>Зараженный</b> и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".                                                              |

► Чтобы проверить функцию Постоянная защита, выполните следующие действия:

1. Загрузите файл eicar.com со страницы сайта EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Сохраните его в папке общего доступа на локальном диске любого из компьютеров сети.

Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

2. Если вы хотите также проверить работу уведомлений пользователей сети, убедитесь в том, что и на защищаемом серверу, и на компьютере, на котором вы сохранили файл eicar.com, включена Служба сообщений Microsoft Windows.
3. Откройте Консоль программы.

4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого сервера одним из следующих способов:
  - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на компьютер, подключившись к сервера помощью программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).
  - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с компьютера, на котором вы его сохранили, через сетевое окружение этого компьютера.

Постоянная защита файлов работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с диска защищаемого сервера.
- В Консоли программы журнал выполнения задачи получил статус **Критический**. В журнале появилась строка с информацией об угрозе в файле eicar.com. (Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Постоянная защита сервера**, выберите задачу Постоянная защита файлов и на панели результатов узла перейдите по ссылке **Открыть журнал выполнения**).
- Появилось сообщение Службы сообщений Microsoft Windows на компьютере, с которого вы скопировали файл следующего содержания:

Kaspersky Security для Windows Server заблокировал доступ к <путь к файлу eicar.com на компьютере>\eicar.com на компьютере <сетевое имя компьютера> в <время возникновения события>. Причина: Обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя объекта: <имя пользователя>. Имя компьютера пользователя объекта: <сетевое имя компьютера, с которого вы скопировали файл>».

Убедитесь, что Служба сообщений Microsoft Windows работает на компьютере, с которого вы скопировали файл eicar.com.

► Чтобы проверить функцию Проверка по требованию, выполните следующие действия:

1. Загрузите файл eicar.com со страницы сайта EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Сохраните его в папке общего доступа на локальном диске любого из компьютеров сети.

Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

2. Откройте Консоль программы.
3. Выполните следующие действия:
  - a. В дереве Консоли программы разверните узел **Проверка по требованию**.
  - b. Выберите вложенный узел **Проверка важных областей**.
  - c. На закладке **Настройка области проверки** откройте контекстное меню на узле **Сетевое окружение** и выберите **Добавить сетевой файл**.
  - d. Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention).
  - e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.



- f. Запустите задачу Проверка важных областей.

Проверка по требованию работает должным образом, если выполняются следующие условия:

- Файл eiscar.com удален с жестких дисков компьютера.
- В Консоли программы журнал выполнения задачи получил статус **Критический**; в журнале выполнения задачи Проверка важных областей появилась строка с информацией об угрозе в файле eiscar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Проверка по требованию**, выберите вложенный узел Проверка важных областей и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

# Проверка целостности компонентов программы

Программа Kaspersky Security для Windows Server содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько модулей или файлов программы модулями или файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов программы, в Kaspersky Security для Windows Server предусмотрена проверка целостности компонентов программы. Программа проверяет модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Целостность компонентов программы проверяется с помощью инструмента `integrity_check_tool`, использующего для проверки файл манифеста – `integrity_check_manifest.xml`, защищенный криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами Администратора.

Инструмент поставляется отдельно от Kaspersky Security для Windows Server на сертифицированном CD-диске.

Инструмент проверки целостности рекомендуется запускать с сертифицированного CD-диска, чтобы гарантировать целостность самого инструмента. При запуске инструмента с CD-диска необходимо указать полный путь к файлу манифеста в директории программы.

► Чтобы проверить целостность компонентов программы, выполните следующие действия:

1. Задайте папку установки Kaspersky Security для Windows Server через пользовательскую переменную окружения при помощи следующей команды:

```
set ProductRoot=<путь к папке>
```

где `<путь к папке>` – это путь к папке установки Kaspersky Security for Windows Server.

По умолчанию используются следующие папки установки:

- В 32-х разрядной версии Microsoft Windows: `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\`.
- В 64-х разрядной версии Microsoft Windows: `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\`

2. Запустите проверку при помощи следующей команды:

```
integrity_check_tool.exe --verify --manifest <путь к файлу>
```

где `<путь к файлу>` – это путь к файлу манифеста – `integrity_check_manifest.xml`. Параметр задается в кавычках.

Инструмент проверки целостности можно запустить со следующими дополнительными параметрами:

- `-h, --help` – показать справку для параметров инструмента.
- `-V, --verbose` – применить вывод расширенной информации о выполненных действиях и результатах. Если вы не укажете этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `-L, --log-file <file>`, где `<file>` – это имя файла, используемое для записи событий, произошедших во время проверки. По умолчанию события передаются в стандартный поток `stdout`.
- `-l, --log-level <0-1000>`, где `<0-1000>` – это уровень детализации вывода событий. По умолчанию уровень детализации – 0.

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

# Разделение доступа к функциям программы по пользовательским ролям

Этот раздел содержит информацию о правах на управление Kaspersky Security для Windows Server и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

## В этом разделе

|                                                                                                                      |                     |
|----------------------------------------------------------------------------------------------------------------------|---------------------|
| О правах на управление Kaspersky Security для Windows Server .....                                                   | <a href="#">278</a> |
| О правах на управление службой Kaspersky Security Service .....                                                      | <a href="#">281</a> |
| О правах доступа к службе Kaspersky Security Management Service .....                                                | <a href="#">96</a>  |
| Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service..... | <a href="#">96</a>  |
| Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля.....                                | <a href="#">286</a> |
| Разрешение сетевых соединений для службы Kaspersky Security Management Service .....                                 | <a href="#">100</a> |

## О правах на управление Kaspersky Security для Windows Server

По умолчанию доступ ко всем функциям Kaspersky Security для Windows Server имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, пользователи группы KAVWSEE Administrators, созданной на защищаемом сервере при установке Kaspersky Security для Windows Server, а также группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Security для Windows Server, могут предоставлять доступ к функциям Kaspersky Security для Windows Server другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Security для Windows Server, он не может открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security для Windows Server один из следующих предустановленных уровней доступа к функциям Kaspersky Security 10 для Windows Server:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Security для Windows Server, параметры работы компонентов Kaspersky Security для Windows Server, права пользователей Kaspersky Security для Windows Server, а также просматривать статистику работы Kaspersky Security 10 для Windows Server.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Security для Windows Server, параметры работы компонентов Kaspersky Security для Windows Server.

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Security для Windows Server, параметры работы компонентов Kaspersky Security для Windows Server, статистику работы Kaspersky Security для Windows Server и права пользователей Kaspersky Security для Windows Server.

Также вы можете выполнять расширенную настройку прав доступа (см. раздел "Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service" на стр. [96](#)): разрешать или запрещать доступ к отдельным функциям Kaspersky Security для Windows Server.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Table 7. Права доступа к функциям Kaspersky Security для Windows Server

| Права доступа             | Описание                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Управление задачами       | Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                           |
| Создание и удаление задач | Возможность создавать и удалять задачи проверки по требованию.                                                                                                                                                                                                                                                                                                                  |
| Изменение параметров      | Возможности: <ul style="list-style-type: none"> <li>• Импортировать из конфигурационного файла параметры работы Kaspersky Security для Windows Server.</li> <li>• Редактировать настройки программы.</li> </ul>                                                                                                                                                                 |
| Чтение параметров         | Возможности: <ul style="list-style-type: none"> <li>• просматривать общие параметры работы Kaspersky Security для Windows Server и параметры задач;</li> <li>• экспортировать в конфигурационный файл параметры работы Kaspersky Security для Windows Server;</li> <li>• просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.</li> </ul> |
| Управление хранилищами    | Возможности: <ul style="list-style-type: none"> <li>• помещать объекты на карантин;</li> <li>• удалять объекты из карантина и резервного хранилища;</li> <li>• восстанавливать объекты из карантина и резервного хранилища.</li> </ul>                                                                                                                                          |
| Управление журналами      | Возможность удалять журналы выполнения задач и очищать журнал системного аудита.                                                                                                                                                                                                                                                                                                |
| Чтение журналов           | Возможность просматривать события в журналах выполнения задач и журнале системного аудита.                                                                                                                                                                                                                                                                                      |
| Чтение статистики         | Возможность просматривать статистику работы каждой задачи Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                |
| Лицензирование программы  | Возможность активировать и деактивировать Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                |
| Удаление программы        | Возможность удалять Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                                      |
| Чтение прав               | Возможность просматривать список пользователей Kaspersky Security для Windows Server и права доступа каждого пользователя.                                                                                                                                                                                                                                                      |

| Права доступа  | Описание                                                                                                                                                                                                                                         |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Изменение прав | <p>Возможности:</p> <ul style="list-style-type: none"> <li>• изменять список пользователей, имеющих доступ к управлению программой;</li> <li>• изменять права доступа пользователей к функциям Kaspersky Security для Windows Server.</li> </ul> |

## О правах на управление службой Kaspersky Security Service

При установке Kaspersky Security для Windows Server регистрирует в Windows службу Kaspersky Security Service (KAVFS), так как программа включает в себя функциональные компоненты, запускаемые при старте операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности на защищаемом сервере через управление Kaspersky Security Service, вы можете ограничивать права на управление службой Kaspersky Security Service с помощью локальной Консоли программы или плагина управления Kaspersky Security Center.

По умолчанию доступ к управлению службой Kaspersky Security Service имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Вы не можете удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи пользователя SYSTEM были изменены, при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, которые имеют доступ с правом на изменение к функциям (см. раздел "О правах на управление Kaspersky Security для Windows Server" на стр. 278), могут предоставлять доступ к управлению службой Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security для Windows Server один из следующих предустановленных уровней доступа на управление службой Kaspersky Security Service:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service, а также запускать и останавливать работу Kaspersky Security Service.
- **Чтение** – возможность просматривать общие параметры работы и права пользователей Kaspersky Security Service.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service.
- **Исполнение** – возможность запускать и останавливать работу Kaspersky Security Service.

Также вы можете выполнять расширенную настройку прав доступа: давать или ограничивать права на управление Kaspersky Security для Windows Server (см. таблицу ниже).

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Table 8. Разграничение прав доступа к функциям Kaspersky Security для Windows Server

| Функция                                                | Описание                                                                                                                                                                                                     |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Чтение настроек службы                                 | Возможность просматривать общие параметры работы и права пользователей Kaspersky Security Service.                                                                                                           |
| Запрос статуса службы у Диспетчера управления службами | Возможность запрашивать статус выполнения Kaspersky Security Service у Диспетчера управления службами Microsoft Windows.                                                                                     |
| Запрос статуса у службы                                | Возможность запрашивать статус выполнения службы у Kaspersky Security Service.                                                                                                                               |
| Перечисление зависимых служб                           | Возможность просматривать список служб, от которых зависит Kaspersky Security Service, а также служб, зависимых от Kaspersky Security Service.                                                               |
| Изменение параметров службы                            | Возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service.                                                                                                |
| Запуск службы                                          | Возможность запускать выполнение Kaspersky Security Service.                                                                                                                                                 |
| Остановка службы                                       | Возможность останавливать выполнение Kaspersky Security Service.                                                                                                                                             |
| Приостановка / Возобновление службы                    | Возможность приостанавливать и возобновлять выполнение Kaspersky Security Service.                                                                                                                           |
| Чтение прав                                            | Возможность просматривать список пользователей Kaspersky Security Service и права доступа каждого пользователя.                                                                                              |
| Изменение прав                                         | Возможности: <ul style="list-style-type: none"> <li>• добавлять и удалять пользователей Kaspersky Security Service;</li> <li>• изменять права доступа пользователей к Kaspersky Security Service.</li> </ul> |
| Удаление службы                                        | Возможность разрегистрации Kaspersky Security Service в Диспетчере управления службами Microsoft Windows.                                                                                                    |
| Пользовательские запросы к службе                      | Возможность создавать и отправлять пользовательские запросы к Kaspersky Security Service.                                                                                                                    |

## О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Security для Windows Server.

При установке Kaspersky Security для Windows Server регистрирует службу управления программой Kaspersky Security для Windows Server (KAVFSGT). Для управления программой через Консоль программы, установленную на другом компьютере требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Security для Windows Server имела полный доступ к Kaspersky Security Management Service на защищаемом сервере.

По умолчанию доступ к управлению службой Kaspersky Security Management Service имеют пользователи, входящие в группу "Администраторы" на защищаемом сервере, и пользователи группы KAVWSEE Administrators, созданной на защищаемом сервере при установке Kaspersky Security для Windows Server.

Вы можете управлять службой Kaspersky Security Management Service только через оснастку **Службы** Microsoft Windows.

Вы не можете разрешать или запрещать пользователям доступ к Kaspersky Security Management Service, настраивая параметры Kaspersky Security для Windows Server.

Вы можете соединиться с Kaspersky Security для Windows Server под локальной учетной записью, если на защищаемом сервере зарегистрирована учетная запись с таким же именем и с таким же паролем.

## Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security Service

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Security для Windows Server и управлению службой Kaspersky Security Service, а также изменять права доступа этих пользователей и групп пользователей.

► Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.



- Если вы хотите настроить параметры программы для одного сервера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел **"Настройка локальных задач в окне Параметры программы в Kaspersky Security Center"** на стр. [129](#)) в Kaspersky Security Center.

3. В разделе **Дополнительные возможности** выполните одно из следующих действий:

- Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
- Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security Service.

Откроется окно **Разрешения для группы "Kaspersky Security для Windows Server"**.

4. В открывшемся окне выполните следующие действия:

- Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
- Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

5. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server которой вы хотите настроить параметры программы.

2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Если вы хотите настроить параметры политики, в Консоли администрирования Kaspersky Security Center в группе серверов выберите закладку **Политики** и откройте **<Имя политики> → Параметры**.
- Если вы хотите настроить параметры программы для одного сервера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел **"Настройка локальных задач в окне Параметры программы в Kaspersky Security Center"** на стр. [129](#)) в Kaspersky Security Center.

3. В разделе **Дополнительные возможности** выполните одно из следующих действий:

- Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
- Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security Service.

Откроется окно **Разрешения для группы "Kaspersky Security для Windows Server"**.

4. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.

5. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
  - **Полный контроль:** полный набор прав на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service.
  - **Чтение:**
    - следующие права на управление Kaspersky Security для Windows Server: **Чтение статистики, Чтение параметров, Чтение журналов и Чтение прав;**
    - следующие права на управление службой Kaspersky Security Service: **Чтение параметров службы, Запрос статуса службы у Диспетчера управления службами, Запрос статуса у службы, Перечисление зависимых служб, Чтение прав.**
  - **Изменение:**
    - все права на управление Kaspersky Security для Windows Server, кроме **Изменения прав;**
    - следующие права на управление службой Kaspersky Security Service: **Изменение параметров службы, Чтение прав.**
  - **Исполнение:** следующие права на управление службой Kaspersky Security Service: **Запуск службы, Остановка службы, Приостановка / Возобновление службы, Чтение прав, Пользовательские запросы к службе.**
6. Если вы хотите выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
  - a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Security для Windows Server** выберите нужного пользователя или группу.
  - b. Нажмите на кнопку **Изменить**.
  - c. В открывшемся окне перейдите по ссылке **Показать особые разрешения**.
  - d. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить или Запретить**).
  - e. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
  - f. Нажмите на кнопку **ОК**.
  - g. В окне **Дополнительные параметры безопасности для Kaspersky Security для Windows Server** нажмите на кнопку **ОК**.
7. В окне **Разрешения для группы "Kaspersky Security для Windows Server"** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Security для Windows Server или службой Kaspersky Security Service будут сохранены.

## Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей (см. раздел "Права доступа к функциям Kaspersky Security для Windows Server" на стр. [278](#)). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Security для Windows Server.

Kaspersky Security для Windows Server запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к локальной Консоли программы;
- удаление Kaspersky Security для Windows Server;
- изменение компонентного состава Kaspersky Security для Windows Server.

Kaspersky Security для Windows Server не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Security для Windows Server хранит заданный пароль в виде контрольной суммы, рассчитанной при задании пароля.

Вы можете экспортировать и импортировать параметры программы, защищенной паролем. Конфигурационный файл, созданный по результатам экспорта параметров защищенной программы, содержит значение контрольной суммы пароля и значение модификатора, используемого для удлинения строки пароля.

Не изменяйте значение контрольной суммы или модификатора в конфигурационном файле. Импорты параметров пароля, измененных вручную, может привести к полному блокированию доступа к управлению программой.

► Чтобы защитить доступ к функциям Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
  - Если вы хотите настроить параметры программы для одного сервера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.  
Откроется окно **Параметры безопасности**.
4. В блоке **Настройки пароля** установите флажок **Использовать защиту паролем**.  
Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям Kaspersky Security для Windows Server.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Security для Windows Server будет запрашивать пароль при доступе к защищаемым операциям.

Установленный пароль невозможно восстановить. Утеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого сервера.

Вы можете изменить или сбросить заданный пароль в параметрах программы в любой момент.

► Чтобы сбросить заданный пароль, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для Server которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры политики для группы серверов, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
  - Если вы хотите настроить параметры программы для одного сервера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.  
Откроется окно **Параметры безопасности**.
4. В блоке **Настройки пароля** снимите флажок **Использовать защиту паролем**.  
Поля **Пароль** и **Подтверждение пароля** будут очищены и станут неактивны.
5. Нажмите на кнопку **ОК**.

Защита паролем будет отключена. Kaspersky Security для Windows Server удалит контрольную сумму старого пароля из параметров программы.

## Разрешение сетевых соединений для службы Kaspersky Security Management Service

Названия параметров могут отличаться в разных операционных системах Windows.

- Чтобы разрешить сетевые соединения для службы Kaspersky Security Management Service на защищаемом сервере, выполните следующие действия:
1. На защищаемом сервере под управлением Microsoft Windows Server выберите **Пуск → Панель управления → Безопасность → Брандмауэр Windows**.
  2. В окне **Параметры брандмауэра Windows** выберите пункт **Изменить параметры**.
  3. На закладке **Исключения** в списке предустановленных исключений установите флажки: **COM + Сетевой доступ, Windows Management Instrumentation (WMI) и Remote Administration**.
  4. Нажмите на кнопку **Добавить программу**.
  5. В окне **Добавление программы** выберите файл kavfsgt.exe. Этот файл хранится в папке, которую вы указали в качестве папки назначения при установке Консоли программы.
  6. Нажмите на кнопку **ОК**.
  7. Нажмите на кнопку **ОК** в окне **Параметры брандмауэра Windows**.

Сетевые соединения для службы Kaspersky Security Management Service на защищаемом сервере будут разрешены.

# Интерфейс программы

Вы можете управлять Kaspersky Security для Windows Server с помощью Плагина управления и через локальную Консоль программы.

Действия в интерфейсе локальной Консоли программы описаны в разделе Работа с Консолью программы (см. раздел "Работа с Консолью Kaspersky Security для Windows Server " на стр. [147](#)).

Действия с Плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

# Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Security для Windows Server и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

## В этом разделе

|                                                                                     |                     |
|-------------------------------------------------------------------------------------|---------------------|
| Управление Kaspersky Security для Windows Server из Kaspersky Security Center ..... | <a href="#">103</a> |
| Управление параметрами программы .....                                              | <a href="#">104</a> |
| Создание и настройка политик .....                                                  | <a href="#">116</a> |
| Создание и настройка задач в Kaspersky Security Center .....                        | <a href="#">126</a> |
| Отчеты в Kaspersky Security Center.....                                             | <a href="#">144</a> |

## Управление Kaspersky Security для Windows Server из Kaspersky Security Center

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Security для Windows Server, объединенными в группу администрирования, с помощью Плагина управления Kaspersky Security для Windows Server. Kaspersky Security Center также позволяет отдельно настраивать параметры работы для каждого защищаемого устройства, входящего в группу администрирования.

*Группа администрирования* формируется вручную на стороне Kaspersky Security Center и включает несколько устройств с установленной программой Kaspersky Security для Windows Server, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Security для Windows Server на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Security для Windows Server из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center.** Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center.

С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты сервера, задач контроля активности на устройствах, задач защиты сетевых хранилищ и параметры запуска системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center.** Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.
- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств.** Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.
- **С помощью окна свойств отдельного компьютера.** В окне **Свойства: <Имя защищаемого устройства>** можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Security для Windows Server, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

## Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Security для Windows Server в Kaspersky Security Center Web Console.

### В этом разделе

|                                                                                         |                     |
|-----------------------------------------------------------------------------------------|---------------------|
| Навигация .....                                                                         | <a href="#">104</a> |
| Настройка общих параметров программы в Kaspersky Security Center .....                  | <a href="#">105</a> |
| Настройка параметров карантина и резервного хранилища в Kaspersky Security Center ..... | <a href="#">112</a> |
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы .....                       | <a href="#">113</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| Переход к общим параметрам из политики .....               | <a href="#">105</a> |
| Переход к общим параметрам из окна свойств программы ..... | <a href="#">105</a> |



## Переход к общим параметрам из политики

► Чтобы открыть параметры программы Kaspersky Security для Windows Server из политики, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. Нажмите на кнопку **Настройка** для группы параметров, которую вы хотите настроить.

## Переход к общим параметрам из окна свойств программы

► Чтобы открыть окно свойств Kaspersky Security для Windows Server для отдельного защищаемого устройства, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
  - двойным щелчком мыши на имени защищаемого устройства;
  - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Security для Windows Server**.
6. Нажмите на кнопку **Свойства**.  
Откроется окно **Параметры программы Kaspersky Security для Windows Server**.
7. Перейдите в раздел **Параметры программы**.

## Настройка общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Security для Windows Server из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

## В этом разделе

|                                                                           |                     |
|---------------------------------------------------------------------------|---------------------|
| Настройка масштабируемости и интерфейса в Kaspersky Security Center ..... | <a href="#">106</a> |
| Настройка параметров безопасности в Kaspersky Security Center .....       | <a href="#">107</a> |
| Настройка параметров соединения в Kaspersky Security Center .....         | <a href="#">109</a> |
| Настройка запуска по расписанию локальных системных задач .....           | <a href="#">110</a> |

## Настройка масштабируемости и интерфейса в Kaspersky Security Center

► Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в подразделе **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
5. В окне **Дополнительные параметры программы** на закладке **Общие** настройте следующие параметры:
  - В разделе **Параметры масштабируемости** настройте параметры, определяющие количество процессов, которые использует Kaspersky Security для Windows Server:
    - **Определять параметры масштабируемости автоматически**  
Kaspersky Security для Windows Server контролирует количество используемых процессов автоматически.  
Это значение установлено по умолчанию.
    - **Указать количество рабочих процессов вручную**  
Kaspersky Security для Windows Server контролирует количество активных рабочих процессов в соответствии с указанными значениями.

- **Максимальное количество активных процессов**

Максимальное количество процессов, которые использует Kaspersky Security для Windows Server. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

- **Количество процессов для постоянной защиты**

Максимальное количество процессов, которые используют компоненты задач постоянной защиты сервера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

- **Количество процессов для фоновых задач проверки по требованию**

Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

- В разделе **Взаимодействие с пользователем** настройте отображение Значка области уведомлений в панели задач: снимите или установите флажок **Показывать Значок области уведомлений**.

6. На закладке **Иерархическое хранилище** выберите параметр для доступа к иерархическому хранилищу (см. раздел "Настройка параметров HSM-системы через Плагин управления" на стр. [591](#)).

7. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут сохранены.

## Настройка параметров безопасности в Kaspersky Security Center

► Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в подразделе **Безопасность** нажмите на кнопку **Настройка**.
5. В окне **Параметры безопасности** настройте следующие параметры:

- В разделе **Параметры надежности** настройте параметры восстановления задач Kaspersky Security для Windows Server в случае сбоев в работе программы или аварийного завершения работы программы.
  - **Выполнять восстановление задач**

Флажок включает или выключает восстановление задач Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.

Если флажок установлен, Kaspersky Security для Windows Server автоматически восстанавливает задачи Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.

Если флажок снят, Kaspersky Security для Windows Server не восстанавливает задачи Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.

По умолчанию флажок установлен.
  - **Выполнять восстановление задач проверки по требованию не более (раз)**

Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Security для Windows Server. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.
- В разделе **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на защищаемое устройство со стороны Kaspersky Security для Windows Server при переходе на источник бесперебойного питания:
  - **Не запускать задачи проверки по расписанию**

Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.

Если флажок установлен, Kaspersky Security для Windows Server не запускает задачи проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.

Если флажок снят, Kaspersky Security для Windows Server запускает задачи проверки по расписанию вне зависимости от режима питания.

По умолчанию флажок установлен.
  - **Остановить выполнение задачи проверки**

Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

Если флажок установлен, Kaspersky Security для Windows Server останавливает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

Если флажок снят, Kaspersky Security для Windows Server продолжает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

По умолчанию флажок установлен.
- В разделе **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Security для Windows Server.

6. Нажмите на кнопку **ОК**.

Настроенные параметры безопасности и надежности будут сохранены.

## Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Security для Windows Server к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► Чтобы настроить параметры соединения, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в подразделе **Соединение** нажмите на кнопку **Настройка**.  
Откроется окно **Параметры соединения**.
5. В окне **Параметры соединения** настройте следующие параметры:
  - В разделе **Параметры прокси-сервера** задайте параметры использования прокси-сервера:
    - **Не использовать прокси-сервер**  
Если выбран этот вариант, Kaspersky Security для Windows Server не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
    - **Использовать параметры указанного прокси-сервера**  
Если выбран этот вариант, для соединения с KSN Kaspersky Security для Windows Server использует параметры прокси-сервера, указанные вручную.
  - IP-адрес или символьное имя прокси-сервера и номер порта
  - **Не использовать прокси-сервер для локальных адресов**  
Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Security для Windows Server.  
Если флажок установлен, обращение к устройствам в сети, к которой принадлежит

защищаемое устройство с установленной программой Kaspersky Security для Windows Server, происходит напрямую. Прокси-сервер не используется.

Если флажок снят, для подключения к локальным устройствам используется прокси-сервер.

По умолчанию флажок установлен.

- В разделе **Параметры аутентификации на прокси-сервере** задайте параметры аутентификации:
  - Выберите параметры аутентификации в раскрывающемся списке.
    - **Не использовать аутентификацию** – проверка подлинности не производится. Этот режим выбран по умолчанию.
    - **Использовать NTLM-аутентификацию** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
    - **Использовать NTLM-аутентификацию с именем пользователя и паролем** – проверка подлинности по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
    - **Использовать имя пользователя и пароль** – проверка подлинности с помощью имени пользователя и пароля.
  - Если требуется, укажите имя пользователя и пароль.
- В разделе **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры соединения будут сохранены.

## Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Security для Windows Server будет выполнять

обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если вы исключите защищаемое устройство из группы администрирования, расписание системных задач будет автоматически включено.

► Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.
2. На закладке **Политики** в контекстном меню политики, для которой вы хотите настроить запуск по расписанию системных задач Kaspersky Security для Windows Server для группы защищаемых устройств, выберите пункт **Свойства**.
3. В окне **Свойства: <Имя политики>** выберите раздел **Параметры программы**. В подразделе **Запуск системных задач** нажмите на кнопку **Настройка** и выполните одно из следующих действий:
  - Установите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
  - Снимите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы запретить запуск по расписанию перечисленных задач.

Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.

4. Убедитесь, что настраиваемая политика активна и применена к выбранной группе защищаемых устройств.
5. Нажмите на кнопку **ОК**.

Настроенные параметры запуска по расписанию для выбранных задач будут применены.



## Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

► Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.
5. В окне **Параметры хранилищ** на закладке **Резервное хранилище** настройте следующие параметры резервного хранилища:
  - Чтобы задать папку резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого устройства или введите полный путь к ней.
  - Чтобы задать максимальный размер резервного хранилища, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.
  - Чтобы задать порог свободного места в резервном хранилище, задайте значение для параметра **Максимальный размер резервного хранилища (МБ)**, установите флажок **Порог доступного пространства (МБ)** и укажите минимальный размер свободного места в папке резервного хранилища в мегабайтах.
  - Чтобы задать папку для восстановленных объектов, в разделе **Параметры восстановления** выберите нужную папку на локальном диске защищаемого устройства или введите имя папки и полный путь к ней в поле **Папка, в которую восстанавливаются объекты**.
6. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие параметры карантина:
  - Чтобы изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого устройства.
  - Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.



- Чтобы задать минимальный объем свободного места в карантине, установите флажки **Максимальный размер карантина (МБ)** и **Порог доступного пространства (МБ)**, затем в поле ввода укажите значение в мегабайтах.
- Чтобы изменить папку, в которую восстанавливаются объекты из карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого устройства.

7. Нажмите на кнопку **ОК**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

## Блокировка доступа к сетевым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры хранилища заблокированных узлов.

### В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| О хранилище заблокированных узлов .....                    | <a href="#">113</a> |
| Включение блокировки узлов .....                           | <a href="#">114</a> |
| Настройка параметров хранилища заблокированных узлов ..... | <a href="#">116</a> |

### О хранилище заблокированных узлов

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов, Защита от шифрования для NetApp или Защита от шифрования. Эти компоненты обнаруживают попытки удаленных узлов зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных узлов. Информация о заблокированных узлах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа на защищаемом устройстве или к папкам сетевого хранилища для всех удаленных узлов из списка заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**.
- Для задачи Защита от шифрования: обнаружено вредоносное шифрование со стороны устройства, обращающегося к сетевым файловым ресурсам.
- Для задачи Защита от шифрования для NetApp: обнаружена атака на сетевое хранилище.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает событие *Предупреждение* для блокировки узла. Все попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локально уникальный идентификатор (LUID) атакующего узла добавлен в список заблокированных узлов, Kaspersky Security для Windows Server определяет IP-адрес этого узла и добавляет его в список заблокированных узлов вместо локально уникального идентификатора атакующего узла.

По умолчанию Kaspersky Security для Windows Server удаляет заблокированные узлы из списка через 30 минут после добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка заблокированных узлов. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

В случае запрета доступа к управлению хранилищами какому-либо пользователю, хранилище заблокированных узлов останется доступным. Параметры хранилища заблокированных узлов не могут быть изменены, если у пользователя отсутствует разрешение типа **Изменение прав** для управления Kaspersky Security для Windows Server.

## Включение блокировки узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от шифрования
- Защита от шифрования для NetApp

► *Чтобы настроить задачу **Постоянная защита файлов**, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита сервера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.  
Откроется окно **Постоянная защита файлов**.
7. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**, если вы хотите, чтобы программа Kaspersky Security для Windows Server блокировала доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность, во время выполнения задачи **Постоянная защита файлов**.
8. Если задача не была запущена, выберите закладку **Управление задачами**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.

9. В окне **Постоянная защита сервера** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу **Защита от шифрования**, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности в сети**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.  
Откроется окно **Защита от шифрования**.
7. Если задача не была запущена, выберите закладку **Управление задачами**:
  - а. Установите флажок **Запускать задачу по расписанию**.
  - б. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
8. В окне **Защита от шифрования** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу **Защита от шифрования для NetApp**, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Защита сетевых хранилищ**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования для NetApp**.  
Откроется окно **Защита от шифрования для NetApp**.
7. Если задача не была запущена, выберите закладку **Управление задачами**:
  - а. Установите флажок **Запускать задачу по расписанию**.
  - б. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
8. В окне **Защита от шифрования для NetApp** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server блокирует доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность или попытки шифрования.

## Настройка параметров хранилища заблокированных узлов

► Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.  
Откроется окно **Параметры хранилищ**.
5. В разделе **Период блокировки узлов** на закладке **Хранилище заблокированных узлов** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым ресурсам.
6. Нажмите на кнопку **ОК**.

## Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Security для Windows Server на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Security для Windows Server.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Security для Windows Server на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, в Консоли администрирования имеет *активный* статус.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Security для Windows Server. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Security для

Windows Server использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы установили значок , вместо значений параметров, действующих до применения политики. Kaspersky Security для Windows Server не применяет значения параметров активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком ) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры для любой задачи постоянной защиты сервера или защиты сетевых хранилищ, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

## В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| Создание политики .....                                                 | <a href="#">117</a> |
| Разделы параметров политики Kaspersky Security для Windows Server ..... | <a href="#">119</a> |
| Настройка политики .....                                                | <a href="#">124</a> |

## Создание политики

Создание новой политики состоит из следующих этапов:

1. Создание политики с помощью мастера создания политик. В окнах мастера можно настроить параметры задач постоянной защиты сервера.
  2. Настройка параметров политики. В окне **Свойства: <Имя политики>** созданной политики вы можете настроить параметры задачи постоянной защиты сервера, общие параметры Kaspersky Security для Windows Server, параметры карантина и резервного хранилища, уровень детализации для журналов выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Security для Windows Server.
- *Чтобы создать политику для группы защищаемых устройств, на которых установлена и запущена программа Kaspersky Security для Windows Server, выполните следующие действия:*
1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для защищаемых устройств которой вы хотите создать политику.
  2. В панели результатов выбранной группы администрирования выберите закладку **Политики** и откройте окно мастера создания политик по ссылке **Создать политику**.
- Откроется окно **Мастер создания политики**.

3. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Security для Windows Server и нажмите на кнопку **Далее**.
4. В поле **Имя** укажите название групповой политики.

Имя политики не должно содержать следующие символы: " \* < : > ? \ | .

5. Чтобы применить параметры политики, используемые в предыдущей версии программы, выполните следующие действия:
  - a. Установите флажок **Использовать параметры политики, созданной для предыдущей версии программы**.
  - b. Нажмите на кнопку **Выбрать**.
  - c. Выберите политику, которую требуется применить.
  - d. Нажмите на кнопку **Далее**.
6. В окне **Выбор типа операции** выберите один из следующих вариантов:
  - **Создать**, чтобы создать политику с заданными по умолчанию параметрами.
  - **Импортировать политику, созданную с помощью предыдущих версий Kaspersky Security для Windows Server**, чтобы использовать импортированную версию политики в качестве шаблона.
  - Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в который вы сохранили параметры ранее созданной политики.
7. В окне **Постоянная защита сервера** настройте задачи и компоненты Постоянная защита файлов, Использование KSN, Защита от эксплойтов и Проверка скриптов. Разрешите или запретите применение настроенных задач политики на защищаемых устройствах сети:
  - Нажмите на кнопку , чтобы разрешить настройку параметров задачи на защищаемых устройствах сети и запретить применение настроенных в политике параметров задачи.
  - Нажмите на кнопку , чтобы запретить настройку параметров задачи на защищаемых устройствах сети и разрешить применение настроенных в политике параметров задачи.

В созданной политике используются заданные по умолчанию параметры задач постоянной защиты сервера.

- Чтобы изменить заданные по умолчанию параметры задачи Постоянная защита файлов, нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.
- Чтобы изменить заданные по умолчанию параметры задачи Использование KSN, нажмите на кнопку **Настройка** в подразделе **Использование KSN**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.

Чтобы запустить задачу Использование KSN, вам нужно принять Положение о KSN в окне **Обработка данных KSN** (см. раздел "Настройка обработки данных" на стр. [355](#)).

- Чтобы изменить заданные по умолчанию параметры компонента Защита от эксплойтов, нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**. В открывшемся окне настройте компонент в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.

8. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:
  - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.
  - **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. Вы сможете активировать эту политику позже.
  - Установите флажок **Открыть свойства политики сразу после создания**, чтобы автоматически закрыть **Мастер создания политики** и настроить новую политику после нажатия на кнопку **Далее**.
9. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик на закладке **Политики** выбранной группы администрирования. В окне **Свойства: <Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Security для Windows Server.

## Разделы параметров политики Kaspersky Security для Windows Server

### Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров для родительских и дочерних политик.

### Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

### Параметры программы

Table 9. Параметры в разделе Параметры программы

| Раздел                              | Параметры                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Масштабируемость и интерфейс</b> | <p>В подразделе <b>Масштабируемость и интерфейс</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• выбрать автоматическую или ручную настройку параметров масштабирования;</li> <li>• настроить параметры отображения значка программы.</li> </ul> |



|                               |                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Безопасность</b>           | <p>В подразделе <b>Безопасность</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• настроить параметры запуска задачи.</li> <li>• указать действия программы при переходе защищаемого устройства на источник бесперебойного питания;</li> <li>• включить или выключить защиту функций программы паролем.</li> </ul> |
| <b>Соединение</b>             | <p>В подразделе <b>Соединение</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN:</p> <ul style="list-style-type: none"> <li>• указать параметры использования прокси-сервера;</li> <li>• указать параметры аутентификации на прокси-сервере.</li> </ul>                          |
| <b>Запуск системных задач</b> | <p>В подразделе <b>Запуск системных задач</b> по кнопке <b>Настройка</b> можно разрешить или запретить запуск следующих системных задач по расписанию, настроенному на защищаемых устройствах:</p> <ul style="list-style-type: none"> <li>• задачи проверки по требованию;</li> <li>• задачи обновления и копирования обновлений.</li> </ul>                                          |

#### Дополнительные возможности

Table 10. Параметры в разделе *Дополнительные возможности*

| Раздел                                                              | Параметры                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Доверенная зона</b>                                              | <p>В подразделе <b>Доверенная зона</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры применения доверенной зоны:</p> <ul style="list-style-type: none"> <li>• сформировать список исключений доверенной зоны;</li> <li>• включить или выключить проверку операций резервного копирования файлов;</li> <li>• сформировать список доверенных процессов.</li> </ul> |
| <b>Проверка съемных дисков</b>                                      | <p>В подразделе <b>Проверка съемных дисков</b> по кнопке <b>Настройка</b> вы можете настроить параметры проверки съемных дисков, подключаемых по USB.</p>                                                                                                                                                                                                                             |
| <b>Права пользователей на управление программой</b>                 | <p>В подразделе <b>Права пользователей на управление программой</b> вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Security для Windows Server.</p>                                                                                                                                                                                |
| <b>Права пользователей на управление службой Kaspersky Security</b> | <p>В подразделе <b>Права пользователей на управление службой Kaspersky Security</b> вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.</p>                                                                                                                                                                            |



|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Хранилища</b> | <p>В подразделе <b>Хранилища</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов:</p> <ul style="list-style-type: none"> <li>указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;</li> <li>настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;</li> <li>указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;</li> <li>настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования.</li> <li>настроить продолжительность блокировки узлов.</li> </ul> |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Постоянная защита сервера

Table 11. Параметры в разделе Постоянная защита сервера

| Раздел                          | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Постоянная защита файлов</b> | <p>В подразделе <b>Постоянная защита файлов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>указать режим защиты объектов;</li> <li>настроить применение эвристического анализатора;</li> <li>настроить применение доверенной зоны;</li> <li>указать область защиты;</li> <li>задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;</li> <li>настроить параметры запуска задачи.</li> </ul> |
| <b>Использование KSN</b>        | <p>В подразделе <b>Использование KSN</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>указать действия над объектами, недоверенными в KSN;</li> <li>настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.</li> </ul> <p>Нажмите на кнопку <b>Обработка данных</b>, чтобы принять или отклонить Положение о KSN и Положение о KMP, а также настроить параметры передачи данных.</p>                                                                   |
| <b>Защита трафика</b>           | <p>В подразделе <b>Защита трафика</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>Настройте режим работы задачи.</li> <li>Настройте антивирусную защиту.</li> <li>Включите защиту от почтовых угроз, антифишинговую проверку и проверку веб-адресов.</li> </ul> <p>Нажмите на <b>Список правил</b>, чтобы настроить правила веб-контроля или применить стандартные правила категоризации.</p>                                                                                                    |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Защита от эксплойтов</b> | <p>В подразделе <b>Защита от эксплойтов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>• выбрать режим защиты памяти процессов;</li> <li>• указать действия для снижения рисков эксплуатации уязвимостей;</li> <li>• дополнить и изменить список защищаемых процессов.</li> </ul>                                                            |
| <b>Проверка скриптов</b>    | <p>В подразделе <b>Проверка скриптов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры запуска задач:</p> <ul style="list-style-type: none"> <li>• разрешить или запретить исполнение предположительно опасных скриптов;</li> <li>• настроить использование эвристического анализатора;</li> <li>• настроить применение доверенной зоны;</li> <li>• настроить параметры запуска задачи.</li> </ul> |

#### Контроль активности на компьютерах

Table 12. Параметры в разделе Контроль активности на компьютерах

| Раздел                           | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Контроль запуска программ</b> | <p>В подразделе <b>Контроль запуска программ</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>• выбрать режим работы задачи;</li> <li>• настроить параметры контроля повторных запусков программ;</li> <li>• указать область применения правил контроля запуска программ;</li> <li>• настроить использование KSN;</li> <li>• настроить параметры запуска задачи.</li> </ul> |

## Защита сетевых хранилищ

Table 13. Параметры в разделе Защита сетевых хранилищ

| Раздел                                 | Параметры                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Постоянная защита файлов (RPC)</b>  | В подразделе <b>Постоянная защита файлов (RPC)</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>использование эвристического анализатора;</li> <li>параметры подключения сетевого хранилища;</li> <li>области защиты задачи.</li> </ul>                                     |
| <b>Постоянная защита файлов (ICAP)</b> | В подразделе <b>Постоянная защита файлов (ICAP)</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>параметры подключения к службе ICAP;</li> <li>интеграция с другими компонентами;</li> <li>уровень безопасности.</li> </ul>                                                 |
| <b>Защита от шифрования для NetApp</b> | В подразделе <b>Защита от шифрования для NetApp</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>режим работы задачи;</li> <li>использование эвристического анализатора;</li> <li>параметры подключения и аутентификации;</li> <li>исключения из области защиты.</li> </ul> |

## Контроль активности в сети

Table 14. Параметры в разделе Контроль активности в сети

| Раздел                      | Параметры                                                                                                                                                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Защита от шифрования</b> | В подразделе <b>Защита от шифрования</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи: <ul style="list-style-type: none"> <li>настроить область защиты от вредоносного шифрования;</li> <li>настроить параметры запуска задачи.</li> </ul> |

## Диагностика системы

Table 15. Параметры в разделе Диагностика системы

| Раздел                              | Параметры                                                                                                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Мониторинг файловых операций</b> | В подразделе <b>Мониторинг файловых операций</b> можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. |
| <b>Анализ журналов</b>              | В подразделе <b>Анализ журналов</b> можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows.                    |

## Журналы и уведомления

Table 16. Параметры в разделе Журналы и уведомления

| Раздел                                      | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Журналы выполнения задач                    | В подразделе <b>Журналы выполнения задач</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>указать уровень важности регистрируемых событий для выбранных компонентов программы;</li> <li>указать параметры хранения журналов выполнения задач;</li> <li>указать параметры интеграции SIEM-системы с Kaspersky Security Center.</li> </ul>                                                                                                     |
| Уведомления о событиях                      | В подразделе <b>Уведомления о событиях</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>указать параметры уведомления пользователя для событий <i>Обнаружен объект</i>, <i>Обнаружено и заблокировано недоверенное запоминающее устройство</i> и <i>Недоверенный узел в списке</i>;</li> <li>указать параметры уведомления администратора для любого выбранного события из списка событий в разделе <b>Настройка уведомлений</b>.</li> </ul> |
| Взаимодействие с Сервером администрирования | В подразделе <b>Взаимодействие с Сервером администрирования</b> по кнопке <b>Настройка</b> вы можете выбрать типы объектов, информацию о которых Kaspersky Security для Windows Server будет передавать на Сервер администрирования.                                                                                                                                                                                                                                                                       |

Подробную информацию о задачах Защиты сетевых хранилищ см. в документе *Руководство по внедрению Kaspersky Security для Windows Server для защиты сетевых хранилищ*.

## История ревизий

В разделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

## Настройка политики

В окне **Свойства: <Имя политики>** существующей политики можно настроить общие параметры Kaspersky Security для Windows Server, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты сервера, параметры контроля активности на серверах, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Security для Windows Server, права доступа к управлению программой и службой Kaspersky Security.

► Чтобы настроить параметры политики, выполните следующие действия:

- В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.

2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:
  - выбрав пункт **Свойства** в контекстном меню политики;
  - Перейдите по ссылке **Настроить параметры политики** в панели результатов выбранной политики.
  - Двойным щелчком мыши по нужной политике.
4. На закладке **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
  - **Активная политика**, если вы хотите, чтобы политика применялась на всех защищаемых устройствах, входящих в выбранную группу администрирования.
  - **Неактивная политика**, если вы хотите активировать политику позже на всех защищаемых устройствах, входящих в выбранную группу администрирования.

Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Security для Windows Server.

5. В разделах **Уведомления о событиях**, **Параметры программы**, **Дополнительные возможности**, **Журналы и уведомления** и **История ревизий** можно настроить параметры программы (см. таблицу ниже).
6. В разделах **Постоянная защита сервера**, **Контроль активности на серверах**, **Контроль активности в сети** и **Диагностика системы** можно настроить параметры программы, а также параметры запуска программы (см. таблицу ниже).

Вы можете включать и выключать выполнение любой задачи на всех защищаемых устройствах, входящих в группу администрирования, с помощью политики Kaspersky Security Center.

Вы можете настроить применение параметров политики на всех защищаемых устройствах сети для каждого отдельного компонента программы.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут применены в политике.

## Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Security для Windows Server, их создании, настройке параметров выполнения, запуске и остановке.

### В этом разделе

|                                                                                        |                     |
|----------------------------------------------------------------------------------------|---------------------|
| О создании задач в Kaspersky Security Center .....                                     | <a href="#">126</a> |
| Создание задачи в Kaspersky Security Center .....                                      | <a href="#">127</a> |
| Настройка локальных задач в окне Параметры программы в Kaspersky Security Center ..... | <a href="#">129</a> |
| Настройка групповых задач в Kaspersky Security Center .....                            | <a href="#">130</a> |
| Настройка параметров диагностики сбоев в Kaspersky Security Center .....               | <a href="#">139</a> |
| Работа с расписанием задач .....                                                       | <a href="#">141</a> |

## О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Мониторинг целостности файлов на основе эталона
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**;
- для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно выключить расписания локальных системных задач обновления и проверки по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [110](#)) на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

## Создание задачи в Kaspersky Security Center

► Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:

1. Запустите мастер создания задачи одним из следующих способов:
    - Для создания локальной задачи:
      - a. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемое устройство.
      - b. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства и выберите пункт **Свойства**.
      - c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
    - Для создания групповой задачи:
      - a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
      - b. Выберите группу администрирования, для которой требуется создать задачу.
      - c. В панели результатов выберите закладку **Задачи** и выберите пункт **Создать задачу**.
    - Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
      - a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
      - b. Выберите группу администрирования, к которой принадлежат защищаемые устройства.
      - c. Выберите защищаемое устройство или произвольный набор защищаемых устройств.
      - d. В раскрывающемся списке **Выполнить действие** выберите **Создать задачу**.
- Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Security для Windows Server** выберите тип создаваемой задачи.
  3. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно **Параметры**. В зависимости от типа задачи параметры могут различаться.
    - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. [525](#)).
    - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
      - a. Выберите источник обновлений в окне **Источник обновлений**.
      - b. Нажмите на кнопку **Параметры соединения**. Откроется окно **Параметры соединения**.
      - c. В окне **Параметры соединения** выполните следующие действия:  
Укажите режим FTP-сервера для соединения с защищаемым устройством.

Если требуется, измените время ожидания при соединении с источником обновления.

Настройте параметры доступа к прокси-серверу при соединении с источником обновлений.

Укажите местоположение защищаемых устройств, чтобы оптимизировать загрузку обновлений.

- Для создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Параметры обновления модулей программы**.
  - a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.
  - b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Security для Windows Server автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешить перезагрузку операционной системы**.
  - c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Security для Windows Server, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступны новые плановые обновления модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Настройка параметров копирования обновлений**.
  - Для создания задачи Активация программы:
    - a. В окне **Параметры активации программы** укажите файл ключа или код активации, с помощью которого вы хотите активировать программу.
    - b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
  - Создайте задачу Формирование правил контроля запуска программ (см. раздел "Создание задачи Формирование правил контроля запуска программ" на стр. [455](#)).
  - Создайте задачу Формирование правил контроля устройств (см. раздел "Создание правил с помощью задачи Формирование правил контроля устройств" на стр. [Ошибка! Закладка не определена.](#)).
4. Настройте расписание задачи (см. раздел "Настройка расписания запуска задач" на стр. [142](#)). Можно настроить расписание для всех типов задач, кроме Откат обновления баз программы.
  5. Нажмите на кнопку **ОК**.
  6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.
  7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.
  8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы " \* < > ? \ | : ).

Рекомендуется включить в название задачи ее тип (например, Проверка по требованию папок общего доступа).



9. В окне **Завершение создания задачи** установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите, чтобы задача была запущена сразу после создания. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

## Настройка локальных задач в окне Параметры программы в Kaspersky Security Center

► Чтобы настроить локальные задачи или общие параметры программы для отдельного защищаемого устройства в сети, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемое устройство.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
  - двойным щелчком мыши на имени защищаемого устройства;
  - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

Откроется окно **Свойства: <Имя защищаемого устройства>**.

4. Чтобы настроить параметры локальной задачи, выполните следующие действия:
  - а. Перейдите в раздел **Задачи**.
    - В списке задач выберите локальную задачу, параметры которой вы хотите настроить.
    - Откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач.
    - Выберите название задачи и нажмите на кнопку **Свойства**.
    - Выберите пункт **Свойства** в контекстном меню выбранной задачи.Откроется окно **Свойства: <Название задачи>**.
5. Чтобы настроить параметры программы, выполните следующие действия:
  - а. Перейдите в раздел **Программы**.
    - В списке установленных программ выберите программу, которую требуется настроить.
    - Откройте окно параметров программы двойным щелчком мыши на названии программы в списке установленных программ.
    - Выделите название программы в списке установленных программ и нажмите на кнопку **Свойства**.
    - Откройте контекстное меню на названии программы в списке установленных программ и выберите пункт **Свойства**.Откроется окно **Параметры <Название программы>**.

Если программа работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения в окне **Параметры <Название программы>**.

## Настройка групповых задач в Kaspersky Security Center

► Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - Выберите название задачи в списке созданных задач двойным щелчком мыши.
  - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
  - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.

В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

4. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
  - Если вы настраиваете задачу проверки по требованию:
    - a. В разделе **Область проверки** настройте область проверки.
    - b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
  - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
    - a. В разделе **Параметры** настройте параметры источника обновлений и оптимизации дисковой подсистемы.
    - b. По кнопке **Параметры соединения** настройте параметры соединения с источником обновлений.
  - Чтобы настроить задачу Обновление модулей программы, в разделе **Параметры обновления модулей программы** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
  - Чтобы настроить задачу Копирование обновлений, в разделе **Параметры копирования обновлений** укажите состав обновлений и папку назначения.
  - Чтобы настроить задачу Активация программы, в разделе **Параметры активации** примените файл ключа или код активации, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
  - Чтобы настроить задачу автоматического формирования разрешающих правил контроля устройств, в разделе **Параметры** укажите параметры, на основе которых будет сформирован список разрешающих правил.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.
7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.
8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Настраиваемые параметры групповых задач приведены в следующей таблице.

Table 17. Параметры групповых задач Kaspersky Security для Windows Server

| Типы задач Kaspersky Security для Windows Server | Раздел в окне Свойства: <Название задачи> | Параметры задачи                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Формирование правил контроля запуска программ    | <b>Настройка</b>                          | <p>При настройке параметров задачи Формирование правил контроля запуска программ вы можете выбрать способ создания разрешающих правил:</p> <ul style="list-style-type: none"> <li>• <b>Создавать разрешающие правила на основе запущенных программ</b></li> </ul> <p>Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.</p> <p>Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.</p> <p>Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.</p> <p>По умолчанию флажок установлен.</p> <p>Флажок нельзя снять, если в таблице <b>Создавать</b></p> |

| Типы задач<br>Kaspersky Security<br>для Windows Server                                                                                                                                                                                                                      | Раздел в окне<br>Свойства:<br><Название<br>задачи> | Параметры задачи                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                             |                                                    | <p><b>разрешающие правила для программ из папок</b> не выбрана ни одна папка.</p> <ul style="list-style-type: none"> <li>Создавать разрешающие правила для программ из папок</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.</p> | <b>Параметры</b>                                   | <p>Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ:</p> <ul style="list-style-type: none"> <li>Использовать цифровой сертификат</li> <li>Использовать заголовок и отпечаток цифрового сертификата</li> <li>Если сертификат отсутствует, использовать</li> <li>Использовать хеш SHA256</li> <li>Формировать правила для пользователя или группы пользователей</li> </ul> <p>Вы можете настроить параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Security для Windows Server создает по завершении задачи.</p> |
|                                                                                                                                                                                                                                                                             | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>Формирование правил контроля устройств</p>                                                                                                                                                                                                                               | <b>Настройка</b>                                   | <ul style="list-style-type: none"> <li>Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.</li> <li>Настройте параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Security для Windows Server создает по завершении задачи.</li> </ul>                                                                                                                                                                                                         |
|                                                                                                                                                                                                                                                                             | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>Активация программы (см. раздел "Задача Активация программы" на стр. <a href="#">135</a>).</p>                                                                                                                                                                           | <b>Параметры активации</b>                         | Вы можете применить код активации или файл ключа для активации программы или продления срока действия лицензии.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                                                                                                                                                                                                                             | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>Копирование обновлений (см. раздел "Задачи обновления" на стр. <a href="#">136</a>).</p>                                                                                                                                                                                 | <b>Источник обновлений</b>                         | <p>Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве</p>                                                                                                                                                                                                                                                              |

| Типы задач<br>Kaspersky Security<br>для Windows Server                                           | Раздел в окне<br>Свойства:<br><Название<br>задачи>             | Параметры задачи                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                  |                                                                | источника обновлений.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                                  | Окно<br><b>Параметры<br/>соединения</b>                        | В окне <b>Параметры соединения</b> , доступном из раздела <b>Источник обновлений</b> , можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                                                                  | <b>Настройка<br/>параметров<br/>копирования<br/>обновлений</b> | Вы можете указать состав обновлений для копирования.<br>В поле <b>Папка для локального хранения скопированных обновлений</b> укажите путь к папке, в которой Kaspersky Security для Windows Server будет сохранять скопированные обновления.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                                                                                  | <b>Расписание</b>                                              | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Обновление баз<br>программы (см. раздел<br>"Задачи обновления" на<br>стр. <a href="#">136</a> ). | <b>Настройка</b>                                               | В блоке параметров <b>Источник обновлений</b> можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.<br>В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему: <ul style="list-style-type: none"> <li>• <b>Снизить нагрузку на дисковую систему</b></li> <li>• <b>Объем оперативной памяти, используемый для оптимизации (МБ)</b></li> </ul> |
|                                                                                                  | Окно<br><b>Параметры<br/>соединения</b>                        | В окне <b>Параметры соединения</b> , доступном из раздела <b>Источник обновлений</b> , можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Типы задач<br>Kaspersky Security<br>для Windows Server                                                                           | Раздел в окне<br>Свойства:<br><Название<br>задачи>                       | Параметры задачи                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                  | <b>Расписание</b>                                                        | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Обновление модулей<br>программы (см. раздел<br>"Задачи обновления" на<br>стр. <a href="#">136</a> ).                             | <b>Источник<br/>обновлений</b>                                           | Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновлений: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.<br><br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. |
|                                                                                                                                  | Окно<br><b>Параметры<br/>соединения</b>                                  | В блоке параметров <b>Параметры соединения с источниками обновлений</b> можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.                                                                                                                                                                                                                                                                            |
|                                                                                                                                  | <b>Настройка<br/>параметров<br/>обновления<br/>модулей<br/>программы</b> | Вы можете указать действия, которые Kaspersky Security для Windows Server будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Security для Windows Server получать информацию о доступных плановых обновлениях.                                                                                                                                                      |
|                                                                                                                                  | <b>Расписание</b>                                                        | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Параметры проверки по<br>требованию (см. раздел<br>"Создание задачи<br>проверки по требованию"<br>на стр. <a href="#">525</a> ). | <b>Область<br/>проверки</b>                                              | Вы можете сформировать область проверки для задачи проверки по требованию и настроить параметры уровня безопасности.                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                                                                                  | Окно<br><b>Параметры<br/>проверки по<br/>требованию</b>                  | В окне <b>Параметры проверки по требованию</b> , доступном из раздела <b>Область проверки</b> , вы можете выбрать один из стандартных уровней безопасности или настроить уровень безопасности вручную.                                                                                                                                                                                                                                                                                       |
|                                                                                                                                  | <b>Параметры</b>                                                         | В блоке параметров <b>Эвристический анализатор</b> вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка.<br><br>В блоке <b>Интеграция с другими компонентами</b> можно настроить следующие параметры: <ul style="list-style-type: none"> <li>• применение Доверенной зоны в задачах проверки по требованию;</li> </ul>                                                                      |

| Типы задач<br>Kaspersky Security<br>для Windows Server                                                                                                       | Раздел в окне<br>Свойства:<br><Название<br>задачи> | Параметры задачи                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                              |                                                    | <ul style="list-style-type: none"> <li>• применение служб KSN в задачах проверки по требованию;</li> <li>• указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.</li> </ul> |
|                                                                                                                                                              | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                       |
| Проверка целостности программы (на стр. <a href="#">138</a> )                                                                                                | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                       |
| Мониторинг целостности файлов на основе эталона (см. раздел "Настройка задачи Мониторинг целостности файлов на основе эталона" на стр. <a href="#">540</a> ) | <b>Расписание</b>                                  | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                       |

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**.

Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.

## В этом разделе

|                                     |                     |
|-------------------------------------|---------------------|
| Задача Активация программы .....    | <a href="#">135</a> |
| Задачи обновления.....              | <a href="#">136</a> |
| Проверка целостности программы..... | <a href="#">138</a> |

## Задача Активация программы

► Чтобы настроить задачу Активация программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - Выберите название задачи в списке созданных задач двойным щелчком мыши.
  - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
  - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.

В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

4. В разделе **Параметры активации программы** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.  
Настроенные параметры групповых задач будут сохранены.

## Задачи обновления

► Чтобы настроить задачи *Копирование обновлений, Обновление баз программы или Обновление модулей программы*, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - Выберите название задачи в списке созданных задач двойным щелчком мыши.
  - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
  - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.



В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

4. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:

- В разделе **Источник обновлений** настройте параметры источника обновлений и оптимизации дисковой подсистемы.
  - a. В разделе **Источник обновлений** вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача (см. раздел "Указание учетной записи для запуска задачи" на стр. 165).

- b. В разделе **Оптимизация использования дисковой подсистемы** для задачи Обновление баз программы вы можете настроить следующие параметры функции, снижающей нагрузку на дисковую подсистему:

- **Снизить нагрузку на дисковую систему**

Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

Если флажок установлен, функция активна.

По умолчанию флажок снят.

- **Объем оперативной памяти, используемый для оптимизации (МБ)**

Объем оперативной памяти (в МБ), используемый программой для хранения файлов обновлений. По умолчанию задан объем 512 МБ. Минимальный объем составляет 400 МБ.

При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

- Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы

будет работать без оптимизации.

В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- а. Нажмите на кнопку **Параметры соединения** и в открывшемся окне **Параметры соединения** настройте параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
- В разделе **Настройка параметров обновления модулей программы** для задачи Обновление модулей программы вы можете указать действия, которые Kaspersky Security для Windows Server будет совершать при наличии критических обновлений модулей программы или при наличии информации о плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
- В разделе **Параметры копирования обновлений** укажите состав обновлений и папку, в которую будут сохранены обновления, для задачи Копирование обновлений.
5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, контролируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

## Проверка целостности программы

► Чтобы настроить групповую задачу Проверка целостности программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - Выберите название задачи в списке созданных задач двойным щелчком мыши.
  - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
  - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.

В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

4. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу Проверка целостности программы.
5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.  
Настроенные параметры групповых задач будут сохранены.

## Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Security для Windows Server возникла проблема (например, аварийное завершение Kaspersky Security для Windows Server) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Security для Windows Server и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Security для Windows Server не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Security для Windows Server. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).
2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.

- В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы трассировки.

- Настройте уровень детализации отладочной информации.

В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Security для Windows Server сохраняет в файле трассировки.

Вы можете выбрать один из следующих уровней детализации:

- **Критические события** – Kaspersky Security для Windows Server сохраняет в файле трассировки только информацию о критических событиях.
- **Ошибки** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях и ошибках.
- **Важные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
- **Информационные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
- **Вся отладочная информация** – Kaspersky Security для Windows Server сохраняет в файле трассировки всю отладочную информацию.

Уровень детализации, который нужно установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

По умолчанию установлен уровень детализации **Вся отладочная информация**.

Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Table 18. Коды подсистем Kaspersky Security для Windows Server

| Код подсистемы | Название подсистемы                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| *              | Все компоненты.                                                                                                         |
| gui            | Подсистема пользовательского интерфейса, оснастка Kaspersky Security для Windows Server в Microsoft Management Console. |
| ak_conn        | Подсистема интеграции с Агентом администрирования Kaspersky Security Center.                                            |

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| bl        | Управляющий процесс, реализует задачи управления Kaspersky Security для Windows Server. |
| wp        | Рабочий процесс; реализует задачи антивирусной защиты.                                  |
| blgate    | Процесс удаленного управления Kaspersky Security для Windows Server.                    |
| ods       | Подсистема проверки по требованию.                                                      |
| oas       | Подсистема постоянной защиты файлов.                                                    |
| qb        | Подсистема карантина и резервного хранилища.                                            |
| scandll   | Вспомогательный модуль антивирусной проверки.                                           |
| core      | Подсистема базовой антивирусной функциональности.                                       |
| avscan    | Подсистема антивирусной обработки.                                                      |
| avserv    | Подсистема управления антивирусным ядром.                                               |
| prague    | Подсистема базовой функциональности.                                                    |
| updater   | Подсистема обновления баз и модулей программы.                                          |
| snmp      | Подсистема поддержки SNMP протокола.                                                    |
| perfcount | Подсистема счетчиков производительности.                                                |

Параметры трассировки оснастки Kaspersky Security для Windows Server (gui) и Плагина управления для Kaspersky Security Center (ak\_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Security для Windows Server применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Security для Windows Server сохраняет отладочную информацию о работе всех компонентов Kaspersky Security для Windows Server.

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.
  - В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файл дампа.

3. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут применены на защищаемом устройстве.

## Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Security для Windows Server, а также настроить параметры запуска по расписанию.

## В этом разделе

|                                                          |                     |
|----------------------------------------------------------|---------------------|
| Настройка расписания запуска задач .....                 | <a href="#">142</a> |
| Включение и выключение запуска задач по расписанию ..... | <a href="#">143</a> |

## Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

► Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - двойным щелчком мыши по имени задачи;
  - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - a. в списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
    - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
    - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
    - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
    - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
  - b. В поле **Время запуска** укажите время первого запуска задачи.

- с. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [110](#)).

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
  - В блоке **Параметры остановки задачи**:
    - a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
    - b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
  - В блоке **Дополнительные параметры**:
    - a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
    - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
    - c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [129](#).

## Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

- *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.



3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - двойным щелчком мыши по имени задачи;
  - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. Выполните одно из следующих действий:
  - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
  - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

## Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Security для Windows Server доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

### Отчет о статусе компонентов Kaspersky Security для Windows Server

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.



Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

- Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:
  1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
  2. Выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [129](#)).
  3. Выберите раздел **Компоненты**.
  4. Ознакомьтесь с таблицей состояния компонентов.
- Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:
  1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
  2. Выберите закладку **Отчеты**.
  3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.  
Будет сформирован отчет.
  4. Ознакомьтесь со следующими элементами отчета:
    - диаграмма;
    - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
    - детальная таблица, показывающая статус, версию, устройство и группу компонента.

## Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

► Чтобы просмотреть отчет о запрещенных программах в режиме *Только статистика*, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме *Только статистика* (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. [438](#)).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах в режиме тестирования** двойным щелчком мыши. Будет сформирован отчет.
5. Ознакомьтесь со следующими элементами отчета:
  - диаграмма, показывающая десять программ с самым большим количеством заблокированных запусков;
  - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
  - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме *Активный* (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. [438](#)).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши. Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

# Работа с Консолью Kaspersky Security для Windows Server

Этот раздел содержит информацию о Консоли Kaspersky Security для Windows Server и об управлении программой через Консоль программы, установленную на защищаемом устройстве или другом устройстве.

## В этом разделе

|                                                                                                                    |                     |
|--------------------------------------------------------------------------------------------------------------------|---------------------|
| О Консоли Kaspersky Security для Windows Server .....                                                              | <a href="#">147</a> |
| Интерфейс Консоли Kaspersky Security для Windows Server .....                                                      | <a href="#">148</a> |
| Управление Kaspersky Security для Windows Server через Консоль программы, установленную на другом устройстве ..... | <a href="#">153</a> |
| Настройка общих параметров программы в Консоли программы .....                                                     | <a href="#">153</a> |
| Управление задачами Kaspersky Security для Windows Server .....                                                    | <a href="#">160</a> |
| Просмотр состояния защиты и информации о Kaspersky Security для Windows Server .....                               | <a href="#">172</a> |

## О Консоли Kaspersky Security для Windows Server

Консоль Kaspersky Security для Windows Server представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

После установки Консоли программы на другое устройство требуется дополнительная настройка.

Если Консоль программы и Kaspersky Security для Windows Server установлены на разных защищаемых устройствах, принадлежащих к разным доменам, возможны ограничения в передаче информации от Kaspersky Security для Windows Server на Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Security для Windows Server добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Security для Windows Server или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Security для Windows Server только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Можно добавить несколько оснасток Kaspersky Security для Windows Server в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Security для Windows Server.

## Интерфейс Консоли Kaspersky Security для Windows Server

В этом разделе описаны основные элементы интерфейса программы.

### В этом разделе

|                                                          |                     |
|----------------------------------------------------------|---------------------|
| Окно Консоли Kaspersky Security для Windows Server ..... | <a href="#">148</a> |
| Значок области уведомлений в панели задач .....          | <a href="#">152</a> |

## Окно Консоли Kaspersky Security для Windows Server

Консоль Kaspersky Security для Windows Server отображается в дереве Microsoft Management Console в виде узла с именем Kaspersky Security.

После подключения к программе Kaspersky Security для Windows Server, установленной на другом защищаемом устройстве, в название узла добавляется имя защищаемого устройства, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Security <имя защищаемого устройства> как <имя учетной записи>**. При подключении к программе Kaspersky Security для Windows Server, установленной на том же защищаемом устройстве, что и Консоль программы, узел называется **Kaspersky Security**.

### Дерево Консоли

В дереве Консоли программы отображается узел **Kaspersky Security** и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Security** содержит следующие вложенные узлы:

- **Постоянная защита сервера:** управление задачами постоянной защиты и службами KSN. Узел **Постоянная защита сервера** позволяет настраивать следующие задачи:
  - **Постоянная защита файлов**
  - **Проверка скриптов**
  - **Использование KSN**
  - **Защита трафика**
  - **Защита от шифрования**
- **Контроль сервера:** контроль запуска программ, установленных на защищаемом устройстве, а также контроль подключения внешних устройств. Узел **Контроль сервера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**

- **Автоматическое формирование правил:** настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имена задач>** (если есть)

Групповые задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль программы.
- **Диагностика системы:** настройка параметров контроля файловых операций и анализа журнала событий Windows.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Защита сетевых хранилищ:** настройка задач защиты сетевых хранилищ.
  - **Защита RPC-подключаемых сетевых хранилищ**
  - **Защита ICAP-подключаемых сетевых хранилищ**
  - **Защита от шифрования для NetApp**
- **Проверка по требованию:** управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка объектов на карантине**
  - **Проверка целостности программы**
  - **Мониторинг целостности файлов на основе эталона**
  - Пользовательские задачи **<Имена задач>** (если есть)

В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)), созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Обновление:** управление обновлением баз и модулей Kaspersky Security для Windows Server, а также копированием обновлений в папку локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также последней задачей **Откат обновления баз программы**:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

В узле отображаются все пользовательские и групповые задачи обновления (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)), сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Хранилища:** управление параметрами карантина, резервного хранилища и заблокированных узлов.

- **Карантин**
- **Резервное хранилище**
- **Заблокированные узлы**
- **Журналы и уведомления:** управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Security для Windows Server.
  - **Журнал безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование:** добавление и удаление ключей Kaspersky Security для Windows Server, просмотр информации о лицензиях.

## Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Security**, в панели результатов отображается информация о текущем состоянии защиты устройства (см. раздел "Просмотр состояния защиты и информации о Kaspersky Security для Windows Server" на стр. [172](#)), информация о Kaspersky Security для Windows Server и о состоянии защиты функциональных компонентов, а также дата истечения срока действия лицензии.

## Контекстное меню узла Kaspersky Security

С помощью пунктов контекстного меню узла **Kaspersky Security** вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру.** Подключиться к другому устройству (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом устройстве" на стр. [153](#)), чтобы управлять установленной на нем программой Kaspersky Security для Windows Server. Для выполнения этой операции вы можете также воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Security**.
- **Запустить службу / Остановить службу.** Запустить или остановить программу или выбранную задачу (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настроить параметры проверки съемных дисков.** Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. [518](#)), подключенных к защищаемому устройству через USB-порт.
- **Защита от эксплойтов: общие параметры.** Настроить режим защиты от эксплойтов и профилактические действия.
- **Защита от эксплойтов: параметры защиты процессов.** Добавить процессы, которые нужно защитить, и выбрать техники защиты от эксплойтов (см. раздел "Техники защиты от эксплойтов" на стр. [589](#)).
- **Настроить параметры доверенной зоны.** Просмотреть и настроить параметры доверенной зоны (см. раздел "О доверенной зоне" на стр. [562](#)).
- **Изменить права пользователей на управление программой.** Просмотреть и настроить права доступа к функциям Kaspersky Security для Windows Server.
- **Изменить права пользователей на управление службой Kaspersky Security.** Просмотреть и настроить права пользователя на управление службой Kaspersky Security (см. раздел "Настройка

прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security" на стр. [287](#)).

- **Иерархическое хранилище.** Настроить способ доступа к HSM-системе (см. раздел "Настройка параметров HSM-системы в Консоли программы" на стр. [592](#)).
- **Экспортировать параметры.** Сохранить параметры программы в конфигурационный XML-файл (см. раздел "Экспорт параметров" на стр. [167](#)). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры.** Импортировать параметры программы из конфигурационного XML-файла (см. раздел "Импорт параметров" на стр. [168](#)). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях.** Перейти к просмотру информации о Kaspersky Security для Windows Server и текущих доступных обновлениях модулей программы.
- **Обновить.** Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства.** Просмотреть и настроить параметры работы Kaspersky Security для Windows Server или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Security** или кнопкой на панели инструментов.

- **Справка.** Перейти к просмотру справки Kaspersky Security для Windows Server. Выполнение этой операции также доступно в контекстных меню задач программы.

## Панель инструментов и контекстное меню задач Kaspersky Security для Windows Server

Вы можете управлять задачами Kaspersky Security для Windows Server с помощью пунктов контекстного меню каждой задачи в дереве Консоли программы.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Запустить / Остановить.** Запустить или остановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Возобновить / Приостановить.** Возобновить или приостановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты сервера и задач проверки по требованию.
- **Добавить задачу.** Создать новую пользовательскую задачу (см. раздел "Создание и настройка задачи проверки по требованию" на стр. [542](#)). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения.** Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. [250](#)). Операция доступна для всех задач.
- **Удалить задачу.** Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.



- **Шаблоны параметров.** Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. [168](#)). Операция доступна для задачи Постоянная защита файлов и задач проверки по требованию.

## Значок области уведомлений в панели задач

Каждый раз, когда Kaspersky Security для Windows Server автоматически запускается после перезагрузки защищаемого устройства, в области уведомлений панели задач отображается значок области уведомлений . Он отображается по умолчанию, если при установке программы вы установили компонент Значок области уведомлений.

Вид значка области уведомлений отражает текущий статус защиты устройства. Возможны следующие два статуса:

- **активный (цветной значок)**, если выполняется хотя бы одна из задач: Постоянная защита файлов, Контроль запуска программ;
- **неактивный (серый значок)**, если не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ.

Вы можете открыть контекстное меню значка области уведомлений по правой клавише мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон программы (см. таблицу ниже).

Table 19. Команды контекстного меню, отображаемые с помощью значка области уведомлений

| Команда                             | Описание                                                                                                                                                                                                                                                |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Открыть Консоль программы</b>    | Открывает Консоль Kaspersky Security для Windows Server (если она установлена).                                                                                                                                                                         |
| <b>Открыть Диагностическое окно</b> | Открывает Диагностическое окно программы.                                                                                                                                                                                                               |
| <b>О программе</b>                  | Открывает окно О программе с информацией о Kaspersky Security для Windows Server.<br>Если вы зарегистрированы в качестве пользователя Kaspersky Security для Windows Server, окно О программе содержит информацию об установленных срочных обновлениях. |
| <b>Скрыть</b>                       | Скрывает значок области уведомлений в панели задач.                                                                                                                                                                                                     |

Скрытый значок области уведомлений можно отобразить в любое время.

► Чтобы снова отобразить значок области уведомлений,

в Microsoft Windows в меню **Пуск** выберите **Все программы > Kaspersky Security для Windows Server > Значок области уведомлений**.



Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

В общих параметрах Kaspersky Security для Windows Server можно включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки защищаемого устройства.

## Управление Kaspersky Security для Windows Server через Консоль программы, установленную на другом устройстве

Вы можете управлять Kaspersky Security для Windows Server через Консоль программы, которая установлена на удаленном устройстве.

Чтобы управление программой с помощью Консоли Kaspersky Security для Windows Server, установленной на удаленном устройстве, было доступно, убедитесь, что выполняются следующие условия:

- Пользователи Консоли программы на удаленном устройстве добавлены в группу KAVWSEE Administrators на защищаемом устройстве.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management (kavfsgt.exe), если на защищаемом устройстве включен брандмауэр Windows.
- Во время установки Kaspersky Security для Windows Server в окне мастера установки был установлен флажок **Разрешить удаленный доступ**.

Если программа Kaspersky Security для Windows Server на удаленном устройстве защищена паролем, введите пароль для получения доступа к управлению программой через Консоль программы.

## Настройка общих параметров программы в Консоли программы

Общие параметры и параметры диагностики сбоев Kaspersky Security для Windows Server определяют общие условия работы программы. Эти параметры позволяют контролировать количество рабочих процессов, используемых Kaspersky Security для Windows Server, включать восстановление задач Kaspersky Security для Windows Server после их аварийного завершения, вести журнал, включать создание файлов дампов для процессов Kaspersky Security для Windows Server при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров программы недоступна из Консоли программы, если изменение данных параметров запрещено активной политикой Kaspersky Security Center.

► Чтобы настроить параметры работы Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Security** и выполните одно из следующих действий:
  - В панели результатов узла перейдите по ссылке **Свойства программы**.
  - В контекстном меню узла выберите пункт **Свойства**.

Откроется окно **Параметры программы**.

2. В открывшемся окне настройте общие параметры Kaspersky Security для Windows Server согласно вашим требованиям:
  - На закладке **Масштабируемость и интерфейс** можно настроить следующие параметры:
    - В разделе **Параметры масштабируемости**:
      - Максимальное количество активных процессов, которые Kaspersky Security для Windows Server может запустить

Table 20. Максимальное количество активных процессов

| Параметр              | Максимальное количество активных процессов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Описание              | <p>Этот параметр относится к группе <b>Параметры масштабируемости</b> Kaspersky Security для Windows Server. Он устанавливает максимальное количество активных процессов, которые программа может запустить одновременно.</p> <p>Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Kaspersky Security для Windows Server к сбоям. Однако слишком высокое значение этого параметра может снизить общую производительность защищаемого устройства и повысить использование оперативной памяти.</p> <p>В Консоли администрирования Kaspersky Security Center можно настроить параметр <b>Максимальное количество активных процессов</b> только для программы Kaspersky Security для Windows Server, установленной на отдельном защищаемом устройстве (в окне <b>Параметры программы</b>); нельзя изменить этот параметр в свойствах политики для группы защищаемых устройств.</p> |                                            |
| Возможные значения    | 1–8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                            |
| Значение по умолчанию | Программа автоматически управляет масштабируемостью, в зависимости от количества процессоров защищаемого устройства:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                            |
|                       | Количество процессоров                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Максимальное количество активных процессов |
|                       | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 1                                          |
|                       | 1 < количество процессоров < 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2                                          |
|                       | 4 и более                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 4                                          |

- Количество процессов для постоянной защиты сервера

Table 21. Количество процессов для постоянной защиты

| Параметр              | Количество процессов для постоянной защиты                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Описание              | <p>Этот параметр относится к группе <b>Параметры масштабируемости</b> Kaspersky Security для Windows Server.</p> <p>С помощью этого параметра можно задать фиксированное количество процессов, в которых Kaspersky Security для Windows Server будет выполнять задачи постоянной защиты сервера.</p> <p>Более высокое значение повысит скорость проверки объектов в задачах постоянной защиты сервера. Однако, чем больше процессов задействует Kaspersky Security для Windows Server, тем больше будет влияние на общую производительность защищаемого устройства и потребление оперативной памяти.</p> <p>В Консоли администрирования Kaspersky Security Center можно настроить параметр <b>Количество процессов для постоянной защиты</b> только для программы Kaspersky Security для Windows Server, установленной на отдельном защищаемом устройстве (в окне <b>Параметры программы</b>); нельзя изменить этот параметр в свойствах политики для группы защищаемых устройств.</p> |                                            |
| Возможные значения    | <p>Возможные значения: от 1 до N, где N – значение, заданное параметром <b>Максимальное количество активных процессов</b>.</p> <p>Если вы установите значение параметра <b>Количество процессов для постоянной защиты</b> равным максимальному количеству активных процессов, вы снизите влияние Kaspersky Security для Windows Server на скорость обмена данными устройств с защищаемым устройством и таким образом повысите его быстродействие во время постоянной защиты сервера. Однако задачи обновления и задачи проверки по требованию с приоритетом <i>Средний (Normal)</i> будут выполняться в уже запущенных рабочих процессах Kaspersky Security для Windows Server. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени.</p> <p>Задачи проверки по требованию с приоритетом <i>Низкий</i> всегда выполняются в отдельных процессах.</p>                |                                            |
| Значение по умолчанию | Kaspersky Security для Windows Server выполняет масштабирование автоматически в зависимости от количества процессоров защищаемого устройства:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                            |
|                       | Количество процессоров                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Количество процессов для постоянной защиты |
|                       | =1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1                                          |
|                       | >1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2                                          |

- Количество рабочих процессов для фоновых задач проверки по требованию

Table 22. Количество процессов для фоновых задач проверки по требованию

| Параметр              | Количество процессов для фоновых задач проверки по требованию                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Описание              | <p>Этот параметр относится к группе <b>Параметры масштабируемости</b> Kaspersky Security для Windows Server.</p> <p>С помощью этого параметра можно указать максимальное количество процессов, для которых программа будет выполнять задачи проверки по требованию в фоновом режиме.</p> <p>Количество процессов, заданное этим параметром, не входит в общее количество процессов Kaspersky Security для Windows Server, заданное параметром <b>Максимальное количество активных процессов</b>.</p> <p>Например, если вы установите следующие значения:</p> <ul style="list-style-type: none"> <li>• максимальное количество активных процессов – 3;</li> <li>• количество процессов для задач постоянной защиты сервера – 3;</li> <li>• количество процессов для фоновых задач проверки по требованию – 1;</li> </ul> <p>а затем запустите задачи постоянной защиты сервера и одну задачу проверки по требованию в фоновом режиме, общее количество рабочих процессов kavfswp.exe в Kaspersky Security для Windows Server составит 4.</p> <p>В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию.</p> <p>Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.</p> |
| Возможные значения    | 1–4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Значение по умолчанию | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

- В разделе **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач при каждом запуске программы (см. раздел "Значок области уведомлений в панели задач" на стр. [152](#)).
- На закладке **Безопасность и надежность** можно настроить следующие параметры:
  - В разделе **Параметры надежности** укажите количество попыток восстановления задач проверки по требованию после их аварийного завершения.

Table 23. Восстановление задач

| Параметр              | Выполнять восстановление задач                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Описание              | <p>Этот параметр относится к группе <b>Параметры надежности</b> Kaspersky Security для Windows Server. Он включает восстановление задач в случае их аварийного завершения и устанавливает количество попыток восстановления задач проверки по требованию.</p> <p>Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Security для Windows Server пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения.</p> <p>Если восстановление задач выключено, программа не восстанавливает задачи постоянной защиты сервера и проверки по требованию.</p> <p>Если восстановление задач включено, программа пытается восстановить задачи постоянной защиты сервера, пока они не будут успешно запущены, а также пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.</p> |
| Возможные значения    | <p>Включено / выключено.</p> <p>Количество попыток восстановления задач проверки по требованию: 1–10.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Значение по умолчанию | Восстановление задач включено. Количество попыток восстановления задач проверки по требованию: 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- В разделе **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Security для Windows Server при переходе на источник бесперебойного питания.

Table 24. Использование источника бесперебойного питания

| Параметр              | Действия при переходе на источник бесперебойного питания                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Описание              | Этот параметр определяет действия, которые Kaspersky Security для Windows Server выполняет, когда защищаемое устройство переходит на работу от источника бесперебойного питания.                                                                                                                                                                                                           |
| Возможные значения    | <p>Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию.</p> <p>Выполнять или останавливать все выполняемые задачи проверки по требованию.</p>                                                                                                                                                                                             |
| Значение по умолчанию | <p>По умолчанию при работе защищаемого устройства от источника бесперебойного питания Kaspersky Security для Windows Server работает в следующем режиме:</p> <ul style="list-style-type: none"> <li>не запускает задачи проверки по требованию, которые должны быть запущены по расписанию;</li> <li>автоматически останавливает все выполняемые задачи проверки по требованию.</li> </ul> |

- В разделе **Параметры применения пароля** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля" на стр. [289](#)).
- На закладке **Параметры соединения**:

- В разделе **Параметры прокси-сервера** укажите параметры прокси-сервера.
- В разделе **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и данные, необходимые для аутентификации на прокси-сервере.
- В разделе **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.
- На закладке **Диагностика сбоев**:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
    - В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы трассировки.
    - Настройте уровень детализации отладочной информации.

В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Security для Windows Server сохраняет в файле трассировки.

Вы можете выбрать один из следующих уровней детализации:

- **Критические события** – Kaspersky Security для Windows Server сохраняет в файле трассировки только информацию о критических событиях.
- **Ошибки** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях и ошибках.
- **Важные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
- **Информационные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
- **Вся отладочная информация** – Kaspersky Security для Windows Server сохраняет в файле трассировки всю отладочную информацию.

Уровень детализации, требуемый для решения возникших проблем, определяет специалист Службы технической поддержки.

По умолчанию установлен уровень детализации **Вся отладочная информация**.

Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты.

Список кодов компонентов Kaspersky Security для Windows Server, о работе которых программа сохраняет отладочную информацию в файле трассировки. Коды компонентов нужно вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Table 25. Коды подсистем Kaspersky Security для Windows Server

| Код подсистемы | Название подсистемы                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| *              | Все компоненты.                                                                                                         |
| gui            | Подсистема пользовательского интерфейса, оснастка Kaspersky Security для Windows Server в Microsoft Management Console. |
| ak_conn        | Подсистема интеграции с Агентом администрирования Kaspersky Security Center.                                            |
| bl             | Управляющий процесс, реализует задачи управления Kaspersky Security для Windows Server.                                 |
| wp             | Рабочий процесс; реализует задачи антивирусной защиты.                                                                  |
| blgate         | Процесс удаленного управления Kaspersky Security для Windows Server.                                                    |
| ods            | Подсистема проверки по требованию.                                                                                      |
| oas            | Подсистема постоянной защиты файлов.                                                                                    |
| qb             | Подсистема карантина и резервного хранилища.                                                                            |
| scandll        | Вспомогательный модуль антивирусной проверки.                                                                           |
| core           | Подсистема базовой антивирусной функциональности.                                                                       |
| avscan         | Подсистема антивирусной обработки.                                                                                      |
| avserv         | Подсистема управления антивирусным ядром.                                                                               |
| prague         | Подсистема базовой функциональности.                                                                                    |
| updater        | Подсистема обновления баз и модулей программы.                                                                          |
| snmp           | Подсистема поддержки SNMP протокола.                                                                                    |
| perfcount      | Подсистема счетчиков производительности.                                                                                |

Параметры трассировки оснастки Kaspersky Security для Windows Server (gui) и Плагина управления Kaspersky Security для Windows Server для Kaspersky Security Center (ak\_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Security для Windows Server применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Security для Windows Server сохраняет отладочную информацию о работе всех компонентов Kaspersky Security для Windows Server.

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы программа создавала файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
- В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файл дампа памяти.

Kaspersky Security для Windows Server не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Security для Windows Server. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

- 1. Нажмите на кнопку **ОК**.  
Параметры работы Kaspersky Security для Windows Server будут сохранены.

# Управление задачами Kaspersky Security для Windows Server

Этот раздел содержит информацию о задачах Kaspersky Security для Windows Server, их создании, настройке параметров выполнения, запуске и остановке.

## В этом разделе

|                                                                        |                     |
|------------------------------------------------------------------------|---------------------|
| Категории задач Kaspersky Security для Windows Server .....            | <a href="#">160</a> |
| Запуск / приостановка / возобновление / остановка задачи вручную ..... | <a href="#">161</a> |
| Работа с расписанием задач .....                                       | <a href="#">161</a> |
| Использование учетных записей для запуска задач .....                  | <a href="#">164</a> |
| Импорт и экспорт параметров .....                                      | <a href="#">165</a> |
| Использование шаблонов параметров безопасности.....                    | <a href="#">168</a> |

## Категории задач Kaspersky Security для Windows Server

Функции постоянной защиты сервера, контроля сервера, проверки по требованию и обновления Kaspersky Security для Windows Server реализованы в виде задач.

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли программы, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Security для Windows Server: *локальные* и *групповые*.



## Локальные задачи

Локальные задачи выполняются только на том защищаемом устройстве, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи.** Создаются автоматически при установке Kaspersky Security для Windows Server. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.
- **Локальные пользовательские задачи.** В Консоли программы вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

## Групповые задачи

Групповые задачи и задачи для наборов управляемых устройств, созданные через Kaspersky Security Center, отображаются в Консоли программы. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли программы можно только просматривать состояние групповых задач.

## Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты сервера и проверки по требованию.

► *Чтобы запустить / приостановить / возобновить / остановить задачу, выполните следующие действия:*

1. Откройте контекстное меню задачи в Консоли программы.
2. Выберите один из следующих вариантов: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (стр. [247](#)).

После возобновления задачи проверки по требованию Kaspersky Security для Windows Server продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

## Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Security для Windows Server, а также настроить параметры запуска по расписанию.

### В этом разделе

|                                                          |                     |
|----------------------------------------------------------|---------------------|
| Настройка расписания запуска задач .....                 | <a href="#">162</a> |
| Включение и выключение запуска задач по расписанию ..... | <a href="#">163</a> |

## Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
    - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
    - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
    - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
    - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
  - b. В поле **Время запуска** укажите время первого запуска задачи.
  - c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.  
 Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
  - В блоке **Параметры остановки задачи**:
    - a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
    - b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
  - В блоке **Дополнительные параметры**:
    - a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
    - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
    - c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **ОК**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

## Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:
  - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
  - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **ОК**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

## Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

### В этом разделе

|                                                         |                     |
|---------------------------------------------------------|---------------------|
| Об использовании учетных записей для запуска задач..... | <a href="#">164</a> |
| Указание учетной записи для запуска задачи.....         | <a href="#">165</a> |

### Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Security для Windows Server:

- задачи Формирование правил контроля запуска программ и Формирование правил контроля устройств;
- задачи проверки по требованию;
- Задачи обновления

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом устройстве в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной в Windows проверкой подлинности NTLM;
- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к проверяемым объектам (например, к файлам в папках общего доступа на защищаемом устройстве);
- в задаче Формирование правил контроля запуска программ, если после выполнения задачи сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, расположенный в одной из папок общего доступа на защищаемом устройстве).

Вы можете запускать задачи обновления, проверки по требованию и автоматического формирования разрешающих правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Security для Windows Server обращается к папкам общего доступа на другом устройстве в сети, если это устройство зарегистрировано в одном домене с защищаемым устройством. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Security для Windows Server будет обращаться к устройству с правами учетной записи **<имя домена \ имя устройства>**.

Указание учетной записи для запуска задачи

- Чтобы указать учетную запись для запуска задачи, выполните следующие действия:
- 1. В дереве Консоли программы откройте контекстное меню задачи, которую вы хотите запустить с правами определенной учетной записи.
  - 2. Выберите пункт **Свойства**.  
Откроется окно **Параметры задачи**.
  - 3. В открывшемся окне на закладке **Запуск с правами** выполните следующие действия:
    - a. Выберите вариант **Имя пользователя**.
    - b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

Выбранный пользователь должен быть зарегистрирован на защищаемом устройстве или в одном домене с защищаемым устройством.

- c. Подтвердите введенный пароль.
4. Нажмите на кнопку **ОК**.
- Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

В этом разделе приведена информация об экспорте параметров Kaspersky Security для Windows Server или параметров определенных программных компонентов в конфигурационный файл в формате XML и об импорте этих параметров из конфигурационного файла в программу.

В этом разделе

|                                        |                     |
|----------------------------------------|---------------------|
| Об импорте и экспорте параметров ..... | <a href="#">166</a> |
| Экспорт параметров .....               | <a href="#">167</a> |
| Импорт параметров .....                | <a href="#">168</a> |

## Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Security для Windows Server в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Security для Windows Server из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Security для Windows Server, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Security для Windows Server:

- Постоянная защита файлов
- Использование KSN
- Контроль запуска программ
- Формирование правил контроля устройств
- Формирование правил контроля запуска программ
- Задачи проверки по требованию
- Защита трафика
- Проверка скриптов
- Защита ICAP-подключаемых сетевых хранилищ
- Защита RPC-подключаемых сетевых хранилищ
- Защита от шифрования для NetApp
- Мониторинг файловых операций
- Анализ журналов
- Обновление баз и модулей Kaspersky Security для Windows Server
- Карантин
- Резервное хранилище
- Журналы
- Уведомления администратора и пользователей
- Доверенная зона
- Защита от эксплойтов
- Хранилище заблокированных узлов
- Защита паролем

Можно также сохранять общие параметры Kaspersky Security для Windows Server и права учетных записей пользователей в конфигурационный файл.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Security для Windows Server экспортирует все пароли, используемые в программе, например, учетные данные для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Пароли можно импортировать только с помощью программы Kaspersky Security для Windows Server, установленной на этом же защищаемом устройстве, если она не была переустановлена или обновлена.

Нельзя импортировать ранее сохраненные пароли с помощью программы Kaspersky Security для Windows Server, установленной на другом защищаемом устройстве. После импорта параметров на другом защищаемом устройстве нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения, применяемые политикой.

Можно импортировать параметры из конфигурационного файла, содержащего параметры только отдельных компонентов Kaspersky Security для Windows Server (например, созданного в программе Kaspersky Security для Windows Server, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Security для Windows Server изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

**Заблокированные параметры активной политики Kaspersky Security Center при импорте параметров не изменяются.**

## Экспорт параметров

► Чтобы экспортировать параметры в конфигурационный файл, выполните следующие действия:

1. В дереве Консоли программы выполните одно из следующих действий:
  - В контекстном меню узла **Kaspersky Security** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Security для Windows Server.
  - В контекстном меню задачи, параметры которой вы хотите экспортировать, выберите пункт **Экспортировать параметры**, чтобы экспортировать параметры отдельного функционального компонента программы.
  - Чтобы экспортировать параметры компонента Доверенная зона:
    - a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
    - b. Выберите пункт **Настроить параметры доверенной зоны**.  
Откроется окно **Доверенная зона**.
    - c. Нажмите на кнопку **Экспорт**.  
Откроется окно приветствия мастера экспорта параметров.

2. Выполните инструкции, которые предлагает **Мастер экспорта параметров**: задайте имя и путь конфигурационного файла для сохранения параметров.

Указывая путь, вы можете использовать системные переменные окружения, но не можете использовать пользовательские переменные окружения.

**Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует параметры, используемые в политике.**

3. В окне **Экспорт параметров программы завершен** нажмите на кнопку **Заккрыть**.

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

## Импорт параметров

► Чтобы импортировать параметры из сохраненного конфигурационного файла, выполните следующие действия:

1. В дереве Консоли программы выполните одно из следующих действий:
  - В контекстном меню узла **Kaspersky Security** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Security для Windows Server.
  - В контекстном меню задачи, параметры которой вы хотите импортировать, выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.
  - Чтобы импортировать параметры компонента Доверенная зона:
    - a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
    - b. Выберите пункт **Настроить параметры доверенной зоны**.  
Откроется окно **Доверенная зона**.
    - c. Нажмите на кнопку **Импорт**.  
Откроется окно приветствия мастера импорта параметров.
2. Выполните инструкции, которые предлагает **Мастер импорта параметров**: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

После импорта общих параметров или функциональных компонентов Kaspersky Security для Windows Server на защищаемое устройство, будет невозможно восстановить их прежние значения.

3. В окне **Импорт параметров программы завершен** нажмите на кнопку **Заккрыть**.  
Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.
4. В панели инструментов Консоли программы нажмите на кнопку **Обновить**.  
Импортированные параметры отобразятся в окне Консоли программы.

Kaspersky Security для Windows Server не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом защищаемом устройстве или на этом же защищаемом устройстве, после того как на нем была переустановлена или обновлена программа Kaspersky Security для Windows Server. После завершения импорта вам нужно ввести пароли вручную.



## Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Security для Windows Server.

### В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| О шаблонах параметров безопасности .....         | <a href="#">169</a> |
| Создание шаблона параметров безопасности .....   | <a href="#">169</a> |
| Просмотр параметров безопасности в шаблоне ..... | <a href="#">170</a> |
| Применение шаблона параметров безопасности ..... | <a href="#">170</a> |
| Удаление шаблона параметров безопасности .....   | <a href="#">171</a> |

### О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Security для Windows Server.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Security для Windows Server:

- Постоянная защита файлов
- Защита RPC-подключаемых сетевых хранилищ
- Проверка при старте операционной системы
- Проверка важных областей
- Задачи проверки по требованию

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов защищаемого устройства, распространяются на все вложенные узлы. Шаблон родительского узла не применяется к вложенным узлам в следующих случаях:

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел "Применение шаблона параметров безопасности" на стр. [170](#)).
- Если вложенные узлы виртуальные. Вам нужно применить шаблон для каждого виртуального узла отдельно.

### Создание шаблона параметров безопасности

► Чтобы сохранить параметры безопасности узла вручную в шаблон, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для которой вы хотите создать шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.

3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.  
Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите дополнительную информацию о шаблоне.
7. Нажмите на кнопку **ОК**.

Шаблон с набором значений параметров безопасности будет сохранен.

## Просмотр параметров безопасности в шаблоне

- *Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для которой вы хотите просмотреть шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.  
Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Название шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приведен список параметров безопасности, сохраненных в шаблоне.

## Применение шаблона параметров безопасности

- *Чтобы применить параметры безопасности из шаблона к выбранному узлу, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов защищаемого устройства откройте контекстное меню узла или элемента, к которому вы хотите применить шаблон.
4. Выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов защищаемого устройства. На закладке **Уровень безопасности** выбранного узла будет установлено значение **Другой**.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов защищаемого устройства, распространяются на все вложенные узлы.

Если область защиты или область проверки вложенных узлов в дереве файловых ресурсов устройства настраивалась отдельно, параметры безопасности из шаблона, примененного к родительскому узлу, не применяются автоматически к таким вложенным узлам.

► Чтобы применить параметры безопасности из шаблона ко всем выбранным узлам, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем его вложенным узлам.
4. В контекстном меню выберите пункт **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов защищаемого устройства. На закладке **Уровень безопасности** выбранного узла будет установлено значение **Другой**.

## Удаление шаблона параметров безопасности

► Чтобы удалить шаблон параметров безопасности, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для настройки которой больше не требуется использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

Вы можете просмотреть шаблоны параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

Откроется окно **Шаблоны**.

3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Откроется окно подтверждения операции удаления.

5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов в дереве файловых ресурсов устройства, настроенные для этих узлов параметры безопасности сохраняются после удаления шаблона.

## Просмотр состояния защиты и информации о Kaspersky Security для Windows Server

- Чтобы просмотреть информацию о состоянии защиты устройства в Kaspersky Security для Windows Server,

в дереве Консоли программы выберите узел **Kaspersky Security**.

По умолчанию информация в панели результатов Консоли программы обновляется автоматически:

- каждые 10 секунд при локальном подключении;
- каждые 15 секунд при удаленном подключении.

Вы можете обновлять информацию вручную.

- Чтобы вручную обновить информацию в узле **Kaspersky Security**,

в контекстном меню узла **Kaspersky Security** выберите пункт **Обновить**.

В панели результатов Консоли программы отображается следующая информация о программе:

- статус использования Kaspersky Security Network;
- состояние защиты устройства;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля защищаемого устройства;
- данные о лицензии;
- статус интеграции с Kaspersky Security Center: данные сервера с установленной программой Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- **Зеленый цвет.** Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- **Желтый цвет.** Задача не запущена, приостановлена или остановлена. Безопасность может быть под угрозой. Рекомендуется настроить и запустить задачу.
- **Красный цвет.** Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в этом разделе (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В разделе **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *Остановлена* или *Не выполнялась*. Индикатор может принимать следующие значения:

- Зеленый – задача Использование KSN выполняется и запросы репутации веб-адресов отправляются в KSN.
- Желтый – принято одно из Положений, но задача не выполняется или запросы статуса веб-адресов не отправляются в KSN.

## Защита сервера

В разделе **Защита сервера** (см. таблицу ниже) отображается информация о текущем состоянии защиты устройства.

Table 26. Информация о состоянии защиты устройства

| Раздел<br>Защита                             | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор состояния защиты устройства</b> | Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: <ul style="list-style-type: none"> <li>• Зеленый – отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется.</li> <li>• Желтый – компонент Постоянная защита файлов не установлен или задача Проверка важных областей не выполнялась в течение долгого времени.</li> <li>• Красный – задача Постоянная защита файлов не выполняется.</li> </ul> |
| <b>Постоянная защита файлов</b>              | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Обнаружено</b> – количество объектов, обнаруженных программой Kaspersky Security для Windows Server. Например, если программа Kaspersky Security для Windows Server обнаружила одну вредоносную программу в пяти файлах, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ превышает 0, значение выделяется красным цветом.</p>                                                  |
| <b>Проверка важных областей</b>              | <p><b>Дата последней проверки</b> – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз безопасности.</p> <p><i>Не выполнялась</i> – событие, которое возникает, если задача Проверка важных областей выполнялась 30 или более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.</p>                                                                                                                                                                                     |
| <b>Защита трафика</b>                        | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Расширение Outlook</b> – установлено или не установлено.</p>                                                                                                                                                                                                                                                                                                                                                                 |

| Раздел<br>Защита                        | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Защита от<br/>эксплойтов</b>         | <p><b>Статус</b> – текущий статус функции защиты от эксплойтов, например, <i>Используется</i> или <i>Не используется</i>.</p> <p><b>Режим защиты</b> – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: <b>Завершать скомпрометированные процессы</b> или <b>Только статистика</b>.</p> <p><b>Процессов защищено</b> – общее количество процессов, которые были добавлены в область защиты и обрабатываются в соответствии с выбранным режимом.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Резервные<br/>копии<br/>объектов</b> | <p><i>Превышен порог доступного пространства в резервном хранилище</i> – событие, которое возникает, если объем доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Security для Windows Server при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле <b>Используемое пространство</b> выделяется желтым цветом.</p> <p><i>Превышен максимальный размер резервного хранилища</i> – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Security для Windows Server при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле <b>Используемое пространство</b> выделяется красным цветом.</p> <p><b>Объектов в резервном хранилище</b> – количество объектов, находящихся в резервном хранилище.</p> <p><b>Используемое пространство</b> – объем используемого пространства в резервном хранилище.</p> |

## Обновление

В разделе **Обновление** (см. таблицу ниже) отображается информация об актуальности баз и модулей программы.

Table 27. Информация о состоянии баз и модулей Kaspersky Security для Windows Server

| Раздел Обновление                                          | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор состояния<br/>баз и модулей<br/>программы</b> | <p>Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>Зеленый – отображается по умолчанию и означает, что базы программы актуальны и последняя задача Обновление баз программы завершена успешно.</li> <li>Желтый – базы программы устарели или последняя задача Обновление баз программы завершена с ошибкой.</li> <li>Красный – возникло событие <i>Базы программы сильно устарели</i> или <i>Базы программы повреждены</i>.</li> </ul> |

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обновление баз программы и Обновление модулей программы</b> | <p><b>Актуальность баз программы</b> – оценка статуса задачи Обновление баз программы.</p> <p>Параметр может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Базы программы актуальны</b> – базы программы были обновлены не более чем 7 дней назад (по умолчанию).</li> <li>• <b>Базы программы устарели</b> – базы программы были обновлены от 7 до 14 дней назад (по умолчанию).</li> <li>• <b>Базы программы сильно устарели</b> – базы программы были обновлены более чем 14 дней назад (по умолчанию).</li> </ul> <p>Вы можете изменять пороги формирования событий <i>Базы программы устарели</i> и <i>Базы программы сильно устарели</i>.</p> <p><b>Дата выпуска баз программы</b> – дата и время выпуска последнего обновления баз программы. Дата и время указаны в UTC-формате.</p> <p><b>Статус последней завершенной задачи обновления баз программы</b> – дата и время последнего обновления баз программы. Дата и время указаны по местному времени защищаемого устройства. Поле окрашивается в красный цвет, если возникло событие <i>Завершена с ошибкой</i>.</p> <p><b>Доступно обновлений модулей программы</b> – количество обновлений модулей Kaspersky Security для Windows Server, доступных для загрузки и установки.</p> <p><b>Установлено обновлений модулей программы</b> – количество установленных обновлений модулей Kaspersky Security для Windows Server.</p> |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Контроль

В разделе **Контроль** (см. таблицу ниже) отображается информация о задачах Контроль запуска программ, Защита от шифрования.

Table 28. Информация о состоянии контроля защищаемого устройства

| Раздел Контроль                                            | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор состояния контроля защищаемого устройства</b> | <p>Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• Зеленый – отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в активном режиме.</li> <li>• Желтый – задача Контроль запуска программ выполняется в режиме Только статистика.</li> <li>• Красный – задача Контроль запуска программ не выполняется или завершена с ошибкой.</li> </ul> |

| Раздел Контроль                  | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Контроль запуска программ</b> | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Режим работы</b> – один из двух доступных режимов работы задачи Контроль запуска программ:</p> <ul style="list-style-type: none"> <li>• <b>Активный</b></li> <li>• <b>Только статистика</b></li> </ul> <p><b>Заблокировано запусков программ</b> – количество попыток запуска программ, заблокированных Kaspersky Security для Windows Server в ходе выполнения задачи Контроль запуска программ. Если количество заблокированных запусков программ превышает 0, поле окрашивается в красный цвет.</p> <p><b>Среднее время обработки (мс)</b> – время, которое потребовалось Kaspersky Security для Windows Server для обработки попытки запуска программ на защищаемом устройстве.</p> |
| <b>Защита от шифрования</b>      | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Режим работы</b> – один из двух доступных режимов работы задачи Защита от шифрования:</p> <ul style="list-style-type: none"> <li>• <b>Активный</b></li> <li>• <b>Только статистика</b></li> </ul> <p><b>Узлов заблокировано</b> – количество узлов, проявивших вредоносную активность и заблокированных при попытке подключения к защищаемому устройству.</p>                                                                                                                                                                                                                                                                                                                           |

## Диагностика

В разделе **Диагностика** (см. таблицу ниже) отображается информация о задачах Мониторинг файловых операций и Анализ журналов.

Table 29. Информация о состоянии диагностики системы

| Раздел Диагностика                   | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор статуса диагностики</b> | <p>Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задачи выполняются.</li> <li>• Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие <i>Не выполняется</i>.</li> <li>• Красный – одна из задач завершена с ошибкой.</li> </ul> |
| <b>Мониторинг файловых операций</b>  | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Несанкционированные файловые операции</b> – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого устройства.</p>                                                                                                                                                                                                                                       |



|                        |                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Анализ журналов</b> | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Возможных нарушений</b> – количество зафиксированных нарушений по данным журнала событий Windows. Это количество определяется на основе заданных правил задачи или применения эвристического анализатора.</p> |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Информация о лицензии на Kaspersky Security для Windows Server отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Security**.

Вы можете настроить свойства Kaspersky Security для Windows Server, перейдя по ссылке **Свойства программы** (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. [153](#)).

Вы можете подключиться к другому защищаемому устройству, перейдя по ссылке **Подключиться к другому компьютеру** (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом устройстве" на стр. [153](#)).

Подробная информация о закладке **Защита сетевых хранилищ** приведена в **Руководстве по внедрению Kaspersky Security для Windows Server для защиты сетевых хранилищ**.

# Работа с Веб-плагином

Этот раздел содержит информацию о Плагине управления Kaspersky Security для Windows Server и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

## В этом разделе

|                                                                                                |                     |
|------------------------------------------------------------------------------------------------|---------------------|
| Управление Kaspersky Security для Windows Server из Kaspersky Security Center Web Console..... | <a href="#">178</a> |
| Ограничения Веб-плагина.....                                                                   | <a href="#">179</a> |
| Управление параметрами программы.....                                                          | <a href="#">179</a> |
| Создание и настройка политик.....                                                              | <a href="#">189</a> |
| Создание и настройка задач в Kaspersky Security Center.....                                    | <a href="#">196</a> |
| Отчеты в Kaspersky Security Center.....                                                        | <a href="#">204</a> |

## Управление Kaspersky Security для Windows Server из Kaspersky Security Center Web Console

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Security для Windows Server, объединенными в группу администрирования, с помощью Веб-плагина Kaspersky Security для Windows Server. Kaspersky Security Center Web Console также позволяет отдельно настраивать параметры работы для каждого защищаемого устройства, входящего в группу администрирования.

*Группа администрирования* формируется вручную на стороне Kaspersky Security Center Web Console и включает несколько устройств с установленной программой Kaspersky Security для Windows Server, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Security для Windows Server на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Security для Windows Server из Kaspersky Security Center Web Console следующими способами:

- **С помощью политик Kaspersky Security Center.** Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне свойств устройства в Kaspersky Security Center Web Console.

С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты сервера, задач контроля активности на устройствах, задач защиты сетевых хранилищ и параметры запуска системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center.** Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.
- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств.** Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.
- **С помощью окна свойств отдельного устройства.** В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Security для Windows Server, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

## Ограничения Веб-плагина

Веб-плагин Kaspersky Security для Windows Server имеет следующие ограничения по сравнению с Плагином управления Kaspersky Security для Windows Server:

- Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
- Для задачи Постоянная защита файлов нельзя изменить стандартный уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. [310](#)).
- Для задачи Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.

## Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Security для Windows Server в Kaspersky Security Center Web Console.

### В этом разделе

|                                                                                   |                     |
|-----------------------------------------------------------------------------------|---------------------|
| Настройка общих параметров программы в Kaspersky Security Center Web Console..... | <a href="#">180</a> |
| Настройка параметров карантина и резервного хранилища с помощью Веб-плагина.....  | <a href="#">185</a> |
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы .....                 | <a href="#">186</a> |

## Настройка общих параметров программы в Kaspersky Security Center Web Console

Вы можете настроить общие параметры Kaspersky Security для Windows Server из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

### В этом разделе

|                                                                                       |                     |
|---------------------------------------------------------------------------------------|---------------------|
| Настройка масштабируемости и интерфейса в Kaspersky Security Center Web Console ..... | <a href="#">180</a> |
| Настройка параметров безопасности в Kaspersky Security Center Web Console .....       | <a href="#">181</a> |
| Настройка параметров соединения в Kaspersky Security Center Web Console.....          | <a href="#">183</a> |
| Настройка запуска по расписанию локальных системных задач .....                       | <a href="#">184</a> |

## Настройка масштабируемости и интерфейса в Kaspersky Security Center Web Console

► *Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Масштабируемость и интерфейс**.
6. Настройте параметры, приведены в следующей таблице.

Table 30. Параметры масштабируемости

| Параметр                                                      | Описание                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Определять параметры масштабируемости автоматически           | Kaspersky Security для Windows Server контролирует количество используемых процессов автоматически.<br>Это значение установлено по умолчанию.                                                                                                       |
| Указать количество рабочих процессов вручную                  | Kaspersky Security для Windows Server контролирует количество активных рабочих процессов в соответствии с указанными значениями.                                                                                                                    |
| Максимальное количество активных процессов                    | Максимальное количество процессов, которые использует Kaspersky Security для Windows Server. Поле ввода доступно, если выбран вариант <b>Указать количество рабочих процессов вручную</b> .                                                         |
| Количество процессов для постоянной защиты                    | Максимальное количество процессов, которые используют компоненты задач постоянной защиты сервера. Поле ввода доступно, если выбран вариант <b>Указать количество рабочих процессов вручную</b> .                                                    |
| Количество процессов для фоновых задач проверки по требованию | Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант <b>Указать количество рабочих процессов вручную</b> . |
| Показывать Значок области уведомлений                         | Настройте, будет ли Значок области уведомлений отображаться в панели задач                                                                                                                                                                          |
| Параметры HSM-системы                                         | Выберите параметр для доступа к иерархическому хранилищу (см. раздел "Настройка параметров HSM-системы через Плагин управления" на стр. <a href="#">591</a> ).                                                                                      |

## Настройка параметров безопасности в Kaspersky Security Center Web Console

► Чтобы вручную настроить параметры безопасности, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Безопасность**.
6. Настройте параметры, приведены в следующей таблице.

Table 31. Параметры безопасности

| Параметр                                                                                              | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Выполнять восстановление задач</b>                                                                 | <p>Флажок включает или выключает восстановление задач Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server автоматически восстанавливает задачи Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не восстанавливает задачи Kaspersky Security для Windows Server после сбоя в работе программы или аварийного завершения работы программы.</p> <p>По умолчанию флажок установлен.</p> |
| Выполнять восстановление задач проверки по требованию не более (раз), значение в диапазоне от 1 до 10 | <p>Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Security для Windows Server. Поле ввода доступно, если установлен флажок <b>Выполнять восстановление задач</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Не запускать задачи проверки по расписанию                                                            | <p>Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server не запускает задачи проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.</p> <p>Если флажок снят, Kaspersky Security для Windows Server запускает задачи проверки по расписанию вне зависимости от режима питания.</p> <p>По умолчанию флажок установлен.</p>                               |
| Остановить выполнение задачи проверки                                                                 | <p>Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server останавливает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.</p> <p>Если флажок снят, Kaspersky Security для Windows Server продолжает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.</p> <p>По умолчанию флажок установлен.</p>                                                                     |
| Использовать защиту паролем                                                                           | <p>Установить пароль для защиты доступа к функциям Kaspersky Security для Windows Server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Настройка параметров соединения в Kaspersky Security Center Web Console

Настроенные параметры соединения используются для подключения Kaspersky Security для Windows Server к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► Чтобы настроить параметры соединения, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Масштабируемость и интерфейс**.
6. Настройте параметры, приведены в следующей таблице.

Table 32. Параметры соединения

| Параметр                                            | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Не использовать прокси-сервер                       | Если выбран этот вариант, Kaspersky Security для Windows Server не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Использовать параметры указанного прокси-сервера    | Если выбран этот вариант, для соединения с KSN Kaspersky Security для Windows Server использует параметры прокси-сервера, указанные вручную.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Не использовать прокси-сервер для локальных адресов | Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Security для Windows Server.<br><br>Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Security для Windows Server, происходит напрямую. Прокси-сервер не используется.<br><br>Если флажок снят, для подключения к локальным устройствам используется прокси-сервер.<br><br>По умолчанию флажок установлен. |
| Параметры аутентификации на прокси-сервере          | Укажите параметры аутентификации                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Не использовать аутентификацию                      | Проверка подлинности не выполняется. Этот режим выбран по умолчанию.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Использовать NTLM-аутентификацию                    | Проверка подлинности выполняется с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Параметр                                                                | Описание                                                                                                                                                     |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Использовать NTLM-аутентификацию с именем пользователя и паролем</b> | Проверка подлинности выполняется по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля. |
| <b>Использовать имя пользователя и пароль</b>                           | Проверка подлинности выполняется с помощью имени пользователя и пароля.                                                                                      |

## Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Security для Windows Server будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если вы исключите защищаемое устройство из группы администрирования, расписание системных задач будет автоматически включено.



► Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Security для Windows Server, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Запуск системных задач**.
6. Настройте параметры, приведены в следующей таблице.

Table 33. Параметры запуска системных задач по расписанию

| Параметр                                                   | Описание                                                                                                                        |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Разрешить запуск задач проверки по требованию              | Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач проверки по требованию              |
| Разрешить запуск задач обновления и копирования обновлений | Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач обновления и копирования обновлений |

## Настройка параметров карантина и резервного хранилища с помощью Веб-плагина

Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Запуск системных задач**.
6. Настройте параметры, приведены в следующей таблице.

Table 34. Параметры запуска системных задач по расписанию

| Параметр                                      | Описание                                         |
|-----------------------------------------------|--------------------------------------------------|
| Папка резервного хранилища                    | Укажите папку резервного хранилища               |
| Максимальный размер резервного хранилища (МБ) | Укажите максимальный размер резервного хранилища |

| Параметр                                          | Описание                                                                   |
|---------------------------------------------------|----------------------------------------------------------------------------|
| <b>Порог доступного пространства (МБ)</b>         | Укажите минимальное значение свободного места в папке резервного хранилища |
| <b>Папка, в которую восстанавливаются объекты</b> | Укажите папку для восстановленных объектов                                 |
| <b>Папка карантина</b>                            | Укажите папку резервного хранилища                                         |
| <b>Максимальный размер карантина (МБ)</b>         | Укажите максимальный размер резервного хранилища                           |
| <b>Порог доступного пространства (МБ)</b>         | Укажите минимальное значение свободного места в папке резервного хранилища |
| <b>Папка, в которую восстанавливаются объекты</b> | Укажите папку для восстановленных объектов                                 |

## Блокировка доступа к сетевым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры хранилища заблокированных узлов.

### В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| О хранилище заблокированных узлов .....                    | <a href="#">186</a> |
| Включение блокировки узлов .....                           | <a href="#">187</a> |
| Настройка параметров хранилища заблокированных узлов ..... | <a href="#">189</a> |

### О хранилище заблокированных узлов

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов, Защита от шифрования для NetApp или Защита от шифрования. Эти компоненты обнаруживают попытки удаленных узлов зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных узлов. Информация о заблокированных узлах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа на защищаемом устройстве или к папкам сетевого хранилища для всех удаленных узлов из списка заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**.
- Для задачи Защита от шифрования: обнаружено вредоносное шифрование со стороны устройства, обращающегося к сетевым файловым ресурсам.
- Для задачи Защита от шифрования для NetApp: обнаружена атака на сетевое хранилище.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает событие *Предупреждение* для блокировки узла. Все попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локально уникальный идентификатор (LUID) атакующего узла добавлен в список заблокированных узлов, Kaspersky Security для Windows Server определяет IP-адрес этого узла и добавляет его в список заблокированных узлов вместо локально уникального идентификатора атакующего узла.

По умолчанию Kaspersky Security для Windows Server удаляет заблокированные узлы из списка через 30 минут после добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка заблокированных узлов. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

В случае запрета доступа к управлению хранилищами какому-либо пользователю, хранилище заблокированных узлов останется доступным. Параметры хранилища заблокированных узлов не могут быть изменены, если у пользователя отсутствует разрешение на изменение прав для управления Kaspersky Security для Windows Server.

## Включение блокировки узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от шифрования
- Защита от шифрования для NetApp

► *Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.

6. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**, если вы хотите, чтобы программа Kaspersky Security для Windows Server блокировала доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность, во время выполнения задачи Постоянная защита файлов.
7. Если задача не была запущена, выберите закладку **Управление задачами**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
8. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу Защита от шифрования, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.  
Откроется окно **Защита от шифрования**.
6. Если задача не была запущена, выберите закладку **Управление задачами**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
7. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу Защита от шифрования для NetApp, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Защита сетевых хранилищ**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования для NetApp**.
6. Откроется окно **Защита от шифрования для NetApp**.
7. Если задача не была запущена, выберите закладку **Управление задачами**:
  - a. Установите флажок **Запускать задачу по расписанию**.
8. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
9. Нажмите на кнопку **Сохранить**.

Kaspersky Security для Windows Server блокирует доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность или попытки шифрования.

## Настройка параметров хранилища заблокированных узлов

► Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Хранилища**.
6. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.  
Откроется окно **Хранилища**.
7. В разделе **Период блокировки узлов** на закладке **Хранилище заблокированных узлов** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым ресурсам.
8. Нажмите на кнопку **ОК**.

## Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Security для Windows Server на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Security для Windows Server.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Security для Windows Server на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, в Консоли администрирования имеет **активный** статус.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Security для Windows Server. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: **Запретить изменение параметров**. После применения политики Kaspersky Security для Windows Server использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы установили значок , вместо значений параметров, действующих до применения политики. Kaspersky Security для Windows Server не применяет значения параметров активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком ) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры для любой задачи постоянной защиты сервера или защиты сетевых хранилищ, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

## В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| Создание политики .....                                                 | <a href="#">190</a> |
| Разделы параметров политики Kaspersky Security для Windows Server ..... | <a href="#">191</a> |

## Создание политики

► Чтобы создать политику, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Нажмите на кнопку **Добавить**.
3. Откроется окно **Новая политика**.
4. В разделе **Выбор программы** выберите Kaspersky Security для Windows Server и нажмите на кнопку **Далее**.
5. На закладке **Общие** вы можете выполнить следующие действия:

- Изменить имя политики.

Имя политики не должно содержать следующие символы: " \* < : > ? \ | .

- Выбрать статус политики:
  - **Активный**. После следующей синхронизации политика будет использоваться на компьютере в качестве активной политики.
  - **Неактивный**. Резервная политика. При необходимости можно перевести неактивную политику в активный статус.
  - **Для автономных пользователей**. Эта политика активируется, когда компьютер покидает периметр сети организации.
- Настроить наследование параметров:
  - **Наследовать параметры родительской политики**. Если включен этот переключатель, значения параметров политики наследуются из политики верхнего уровня. Параметры политики недоступны для изменения, если для родительской политики установлен .
  - **Принудительное наследование параметров в дочерних политиках**. Если переключатель включен, значения параметров политики распространяются на дочерние политики. В параметрах дочерней политики автоматически устанавливается флажок **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из

родительской политики, за исключением параметров, отмеченных . Параметры дочерней политики недоступны для изменения, если для родительской политики установлен .

6. На закладке **Параметры программы** настройте параметры политики в соответствии с вашими требованиями.
7. Нажмите на кнопку **Сохранить**.

Созданная политика отобразится в списке политик на закладке **Политики и профили** выбранной группы администрирования. В окне **<Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Security для Windows Server.

## Разделы параметров политики Kaspersky Security для Windows Server

### Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров для родительских и дочерних политик.

### Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

### Параметры программы

Table 35. Параметры в разделе Параметры программы

| Раздел                              | Параметры                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Масштабируемость и интерфейс</b> | В подразделе <b>Масштабируемость и интерфейс</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>• выбрать автоматическую или ручную настройку параметров масштабирования;</li> <li>• настроить параметры отображения значка программы.</li> </ul>                                                                  |
| <b>Безопасность;</b>                | В подразделе <b>Безопасность</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>• настроить параметры запуска задачи.</li> <li>• указать действия программы при переходе защищаемого устройства на источник бесперебойного питания;</li> <li>• включить или выключить защиту функций программы паролем.</li> </ul> |

|                               |                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Соединение</b>             | <p>В подразделе <b>Соединение</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN:</p> <ul style="list-style-type: none"> <li>указать параметры использования прокси-сервера;</li> <li>указать параметры аутентификации на прокси-сервере.</li> </ul> |
| <b>Запуск системных задач</b> | <p>В подразделе <b>Запуск системных задач</b> по кнопке <b>Настройка</b> можно разрешить или запретить запуск следующих системных задач по расписанию, настроенному на защищаемых устройствах:</p> <ul style="list-style-type: none"> <li>задачи проверки по требованию;</li> <li>задачи обновления и копирования обновлений.</li> </ul>                 |

#### Дополнительные возможности

Table 36. Параметры в разделе *Дополнительные возможности*

| Раздел                                                              | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Доверенная зона</b>                                              | <p>В подразделе <b>Доверенная зона</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры применения доверенной зоны:</p> <ul style="list-style-type: none"> <li>сформировать список исключений доверенной зоны;</li> <li>включить или выключить проверку операций резервного копирования файлов;</li> <li>сформировать список доверенных процессов.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Проверка съемных дисков</b>                                      | <p>В подразделе <b>Проверка съемных дисков</b> по кнопке <b>Настройка</b> вы можете настроить параметры проверки съемных дисков, подключаемых по USB.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Права пользователей на управление программой</b>                 | <p>В подразделе <b>Права пользователей на управление программой</b> вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Security для Windows Server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Права пользователей на управление службой Kaspersky Security</b> | <p>В подразделе <b>Права пользователей на управление службой Kaspersky Security</b> вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Хранилища</b>                                                    | <p>В подразделе <b>Хранилища</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов:</p> <ul style="list-style-type: none"> <li>указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;</li> <li>настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;</li> <li>указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;</li> <li>настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования.</li> <li>настроить продолжительность блокировки узлов.</li> </ul> |



# Постоянная защита сервера

Table 37. Параметры в разделе Постоянная защита сервера

| Раздел                          | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Постоянная защита файлов</b> | <p>В подразделе <b>Постоянная защита файлов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>указать режим защиты объектов;</li> <li>настроить применение эвристического анализатора;</li> <li>настроить применение доверенной зоны;</li> <li>указать область защиты;</li> <li>задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;</li> <li>настроить параметры запуска задачи.</li> </ul> |
| <b>Использование KSN</b>        | <p>В подразделе <b>Использование KSN</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>указать действия над объектами, недоверенными в KSN;</li> <li>настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.</li> </ul>                                                                                                                                                                                                                                 |
| <b>Защита трафика</b>           | <p>В подразделе <b>Защита трафика</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>Настройте режим работы задачи.</li> <li>Настройте антивирусную защиту.</li> <li>Включите защиту от почтовых угроз, антифишинговую проверку и проверку веб-адресов.</li> </ul>                                                                                                                                                                                                                                  |
| <b>Защита от эксплойтов</b>     | <p>В подразделе <b>Защита от эксплойтов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>выбрать режим защиты памяти процессов;</li> <li>указать действия для снижения рисков эксплуатации уязвимостей;</li> <li>дополнить и изменить список защищаемых процессов.</li> </ul>                                                                                                                                                                                                                     |
| <b>Проверка скриптов</b>        | <p>В подразделе <b>Проверка скриптов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры запуска задач:</p> <ul style="list-style-type: none"> <li>разрешить или запретить исполнение предположительно опасных скриптов;</li> <li>настроить использование эвристического анализатора;</li> <li>настроить применение доверенной зоны;</li> <li>настроить параметры запуска задачи.</li> </ul>                                                                                                                                                            |

## Контроль активности на компьютерах

Table 38. Параметры в разделе *Контроль активности на компьютерах*

| Раздел                           | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Контроль запуска программ</b> | <p>В подразделе <b>Контроль запуска программ</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>• выбрать режим работы задачи;</li> <li>• настроить параметры контроля повторных запусков программ;</li> <li>• указать область применения правил контроля запуска программ;</li> <li>• настроить использование KSN;</li> <li>• настроить параметры запуска задачи.</li> </ul> |

## Защита сетевых хранилищ

Table 39. Параметры в разделе *Защита сетевых хранилищ*

| Раздел                                 | Параметры                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Постоянная защита файлов (RPC)</b>  | <p>В подразделе <b>Постоянная защита файлов (RPC)</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• использование эвристического анализатора;</li> <li>• параметры подключения сетевого хранилища;</li> <li>• области защиты задачи.</li> </ul>                                       |
| <b>Постоянная защита файлов (ICAP)</b> | <p>В подразделе <b>Постоянная защита файлов (ICAP)</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• параметры подключения к службе ICAP;</li> <li>• интеграция с другими компонентами;</li> <li>• уровень безопасности.</li> </ul>                                                   |
| <b>Защита от шифрования для NetApp</b> | <p>В подразделе <b>Защита от шифрования для NetApp</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• режим работы задачи;</li> <li>• использование эвристического анализатора;</li> <li>• параметры подключения и аутентификации;</li> <li>• исключения из области защиты.</li> </ul> |

## Контроль активности в сети

Table 40. Параметры в разделе *Контроль активности в сети*

| Раздел                      | Параметры                                                                                                                                                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Защита от шифрования</b> | <p>В подразделе <b>Защита от шифрования</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>• настроить область защиты от вредоносного шифрования;</li> <li>• настроить параметры запуска задачи.</li> </ul> |

## Диагностика системы

Table 41. Параметры в разделе Диагностика системы

| Раздел                              | Параметры                                                                                                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Мониторинг файловых операций</b> | В подразделе <b>Мониторинг файловых операций</b> можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. |
| <b>Анализ журналов</b>              | В подразделе <b>Анализ журналов</b> можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows.                    |

## Журналы и уведомления

Table 42. Параметры в разделе Журналы и уведомления

| Раздел                                             | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Журналы выполнения задач</b>                    | В подразделе <b>Журналы выполнения задач</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>указать уровень важности регистрируемых событий для выбранных компонентов программы;</li> <li>указать параметры хранения журналов выполнения задач;</li> <li>указать параметры интеграции SIEM-системы с Kaspersky Security Center.</li> </ul>                                                                                                            |
| <b>Уведомления о событиях</b>                      | В подразделе <b>Уведомления о событиях</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры: <ul style="list-style-type: none"> <li>указать параметры уведомления пользователя для событий <i>Обнаружен объект</i>, <i>Обнаружено и заблокировано</i> <i>недоверенное запоминающее устройство</i> и <i>Недоверенный узел в списке</i>;</li> <li>указать параметры уведомления администратора для любого выбранного события из списка событий в разделе <b>Настройка уведомлений</b>.</li> </ul> |
| <b>Взаимодействие с Сервером администрирования</b> | В подразделе <b>Взаимодействие с Сервером администрирования</b> по кнопке <b>Настройка</b> вы можете выбрать типы объектов, информацию о которых Kaspersky Security для Windows Server будет передавать на Сервер администрирования.                                                                                                                                                                                                                                                                              |

Подробную информацию о задачах Защиты сетевых хранилищ см. в документе *Руководство по внедрению Kaspersky Security для Windows Server для защиты сетевых хранилищ*.

## История ревизий

В разделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

## Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Security для Windows Server, их создании, настройке параметров выполнения, запуске и остановке.

### В этом разделе

|                                                                          |                     |
|--------------------------------------------------------------------------|---------------------|
| О создании задач в Kaspersky Security Center Web Console .....           | <a href="#">196</a> |
| Создание задачи в Kaspersky Security Center Web Console .....            | <a href="#">197</a> |
| Настройка групповых задач в Kaspersky Security Center .....              | <a href="#">198</a> |
| Настройка параметров диагностики сбоев в Kaspersky Security Center ..... | <a href="#">199</a> |
| Работа с расписанием задач .....                                         | <a href="#">202</a> |

## О создании задач в Kaspersky Security Center Web Console

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Мониторинг целостности файлов на основе эталона
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**;
- для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно выключить расписания локальных системных задач обновления и проверки по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [110](#)) на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

## Создание задачи в Kaspersky Security Center Web Console

► Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:

1. Запустите мастер создания задачи одним из следующих способов:
  - Для создания локальной задачи:
    - a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
    - a. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
    - b. Выберите название защищаемого устройства.
    - c. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
    - d. Нажмите на кнопку **Добавить**.
  - Для создания групповой задачи:
    - a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
    - b. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.
    - c. Нажмите на кнопку **Добавить**.
  - Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
    - a. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
    - b. Выберите выборку устройств, для которой требуется создать задачу.
    - c. Нажмите на кнопку **Запустить**.
    - d. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.
    - e. Нажмите на кнопку **Создать задачу**.

Откроется окно мастера создания задачи.

2. В раскрывающемся списке **Программы** выберите **Kaspersky Security для Windows Server**.
3. В раскрывающемся списке **Тип задачи** выберите тип создаваемой задачи.
4. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно параметров. В зависимости от типа задачи параметры могут различаться.
  - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. [525](#)).
  - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
    - a. Выберите источник обновлений в разделе **Источник обновлений**.
    - b. В окне **Параметры соединения** настройте параметры прокси-сервера.

- После создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Обновление модулей программы**:
    - a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.
    - b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Security для Windows Server автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешить перезагрузку операционной системы**.
    - c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Security для Windows Server, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.  
 "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступны новые плановые обновления модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.
  - Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Копирование обновлений**.
  - Для создания задачи Активация программы:
    - a. В окне **Список ключей в хранилище Kaspersky Security Center** укажите файл ключа или код активации, с помощью которого вы хотите активировать программу.
    - b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
  - Создайте задачу Формирование правил контроля запуска программ и настройте ее параметры.
  - Создайте задачу Формирование правил контроля устройств и настройте ее параметры.
5. Нажмите на кнопку **Далее**.
  6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.
  7. Нажмите на кнопку **Далее**.
  8. В окне **Завершение создания задачи** установите флажок **Перейти к параметрам задачи после создания**, чтобы настроить параметры задачи.
  9. Нажмите на кнопку **Готово**.
- Созданная задача отобразится в списке **Задачи**.

## Настройка групповых задач в Kaspersky Security Center

- *Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:*
1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
  2. Щелкните по названию задачи в списке задач Kaspersky Security Center.  
Откроется окно **<Название задачи>**.

3. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
  - Если вы настраиваете задачу проверки по требованию:
    - a. В разделе **Область проверки** настройте область проверки.
    - b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
  - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
    - a. В разделе **Источники обновлений** настройте параметры источника обновлений и прокси-сервера.
    - b. В разделе **Оптимизация** настройте параметры оптимизации дисковой подсистемы.
  - Чтобы настроить задачу Обновление модулей программы, в разделе **Дополнительные параметры** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
  - Чтобы настроить задачу Копирование обновлений, в разделе **Параметры копирования обновлений** укажите состав обновлений и папку назначения.
  - Чтобы настроить задачу Активация программы, примените файл ключа или код активации, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
  - Чтобы настроить автоматическое формирование разрешающих правил контроля устройств, укажите параметры, на основе которых будет сформирован список разрешающих правил.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. На закладке **Параметры** в разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center*.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры групповых задач будут сохранены.

## Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Security для Windows Server возникла проблема (например, аварийное завершение Kaspersky Security для Windows Server) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Security для Windows Server и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Security для Windows Server не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Security для Windows Server. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).
2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
  - В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы трассировки.
  - Настройте уровень детализации отладочной информации.

В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Security для Windows Server сохраняет в файле трассировки.

Вы можете выбрать один из следующих уровней детализации:

- **Критические события** – Kaspersky Security для Windows Server сохраняет в файле трассировки только информацию о критических событиях.
- **Ошибки** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях и ошибках.
- **Важные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
- **Информационные события** – Kaspersky Security для Windows Server сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
- **Вся отладочная информация** – Kaspersky Security для Windows Server сохраняет в файле трассировки всю отладочную информацию.

Уровень детализации, который нужно установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

По умолчанию установлен уровень детализации **Вся отладочная информация**.

Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).



Table 43. Коды подсистем Kaspersky Security для Windows Server

| Код подсистемы | Название подсистемы                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| *              | Все компоненты.                                                                                                         |
| gui            | Подсистема пользовательского интерфейса, оснастка Kaspersky Security для Windows Server в Microsoft Management Console. |
| ak_conn        | Подсистема интеграции с Агентом администрирования Kaspersky Security Center.                                            |
| bl             | Управляющий процесс, реализует задачи управления Kaspersky Security для Windows Server.                                 |
| wp             | Рабочий процесс; реализует задачи антивирусной защиты.                                                                  |
| blgate         | Процесс удаленного управления Kaspersky Security для Windows Server.                                                    |
| ods            | Подсистема проверки по требованию.                                                                                      |
| oas            | Подсистема постоянной защиты файлов.                                                                                    |
| qb             | Подсистема карантина и резервного хранилища.                                                                            |
| scandll        | Вспомогательный модуль антивирусной проверки.                                                                           |
| core           | Подсистема базовой антивирусной функциональности.                                                                       |
| avscan         | Подсистема антивирусной обработки.                                                                                      |
| avserv         | Подсистема управления антивирусным ядром.                                                                               |
| prague         | Подсистема базовой функциональности.                                                                                    |
| updater        | Подсистема обновления баз и модулей программы.                                                                          |
| snmp           | Подсистема поддержки SNMP протокола.                                                                                    |
| perfcoun       | Подсистема счетчиков производительности.                                                                                |

Параметры трассировки оснастки Kaspersky Security для Windows Server (gui) и Плагина управления для Kaspersky Security Center (ak\_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcoun) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Security для Windows Server применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Security для Windows Server сохраняет отладочную информацию о работе всех компонентов Kaspersky Security для Windows Server.

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.
  - В поле ниже укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файл дампа.

3. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут применены на защищаемом устройстве.

## Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Security для Windows Server, а также настроить параметры запуска по расписанию.

### В этом разделе

|                                                          |                     |
|----------------------------------------------------------|---------------------|
| Настройка расписания запуска задач .....                 | <a href="#">202</a> |
| Включение и исключение запуска задач по расписанию ..... | <a href="#">203</a> |

## Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

► Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.  
Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. В разделе **Расписание** установите флажок **Запускать задачу по расписанию**.

Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - а. в списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
    - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
    - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
    - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
    - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

- b. В поле **Время запуска** укажите время первого запуска задачи.
  - c. В поле **Начать с** укажите дату начала действия расписания.
6. В блоке **Параметры остановки задачи**:
- a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
  - b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
7. В блоке **Дополнительные параметры**:
- a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
  - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
  - c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры запуска задачи.

## Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.  
Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. Выберите раздел **Расписание**.
5. Выполните одно из следующих действий:
  - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
  - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

## Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Security для Windows Server доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

### Отчет о статусе компонентов Kaspersky Security для Windows Server

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center Web Console присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Выберите название защищаемого устройства.
3. На закладке **Общие** выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

► Чтобы просмотреть стандартный отчет Kaspersky Security Center Web Console, выполните следующие действия:

1. Выберите **Мониторинг и отчетность** → **Отчеты**.

2. В списке выберите **Отчет о статусе компонентов программы** и нажмите на кнопку **Показать отчет**.

Будет сформирован отчет.

3. Ознакомьтесь со следующими элементами отчета:

- диаграмма;
- итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
- детальная таблица, показывающая статус, версию, устройство и группу компонента.

## Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

- *Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. [438](#)).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.  
Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
  - диаграмма, показывающая десять программ с самым большим количеством заблокированных запусков;
  - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
  - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

- *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. [438](#)).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.  
Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

# Диагностическое окно

В этом разделе описано использование диагностического окна для просмотра статуса или текущей активности защищаемого устройства и настройка записи файлов дампов и файлов трассировки.

## В этом разделе

|                                                                                             |                     |
|---------------------------------------------------------------------------------------------|---------------------|
| О диагностическом окне .....                                                                | <a href="#">206</a> |
| Просмотр состояния Kaspersky Security для Windows Server с помощью диагностического окна .. | <a href="#">207</a> |
| Просмотр статистики событий безопасности .....                                              | <a href="#">208</a> |
| Просмотр текущей активности программы .....                                                 | <a href="#">208</a> |
| Настройка записи файлов дампов и файлов трассировки .....                                   | <a href="#">209</a> |

## О диагностическом окне

Компонент Диагностическое окно (далее также CDI) устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы и может быть использован, даже если Консоль программы не установлена на защищаемом устройстве. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на защищаемом устройстве.

В диагностическом окне можно выполнять следующие действия:

- просматривать информацию об общем состоянии программы (см. раздел "Просмотр состояния Kaspersky Security для Windows Server с помощью диагностического окна" на стр. [207](#));
- просматривать произошедшие инциденты безопасности (см. раздел "Просмотр статистики событий безопасности" на стр. [208](#));
- просматривать текущую активность на защищаемом устройстве (см. раздел "Просмотр текущей активности программы" на стр. [208](#));
- запускать и останавливать запись файлов дампов и файлов трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. [209](#));
- открывать Консоль программы;
- открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Security для Windows Server защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

## Просмотр состояния Kaspersky Security для Windows Server с помощью диагностического окна

► Чтобы открыть диагностическое окно, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

Откроется **Диагностическое окно**.

На закладке **Статус защиты** можно просмотреть текущий статус ключа, а также статус задач постоянной защиты сервера и задач обновления. Для уведомления о состояниях защиты используется цветовая индикация (см. таблицу ниже).

Table 44. Статус защиты в диагностическом окне

| Раздел                             | Состояние                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Состояние постоянной защиты</b> | <p>Панель <i>зеленого</i> цвета отображается при любом из следующих сценариев (при выполнении любого из условий):</p> <ul style="list-style-type: none"> <li>• Рекомендуемая конфигурация: <ul style="list-style-type: none"> <li>• Задача Постоянная защита файлов запущена с параметрами по умолчанию.</li> <li>• Задача Контроль запуска программ запущена в режиме <b>Активный</b> с параметрами по умолчанию.</li> </ul> </li> <li>• Приемлемая конфигурация: <ul style="list-style-type: none"> <li>• Задача Постоянная защита файлов настроена пользователем.</li> <li>• Параметры задачи Контроль запуска программ изменены.</li> </ul> </li> </ul> |
|                                    | <p>Панель <i>желтого</i> цвета отображается, если выполнено одно или несколько из следующих условий:</p> <ul style="list-style-type: none"> <li>• Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию).</li> <li>• Задача Контроль запуска программ запущена в режиме <b>Только статистика</b>.</li> <li>• Защита от эксплойтов и задача Контроль запуска программ запущены в режиме <b>Только статистика</b>.</li> </ul>                                                                                                                                                                                                 |
|                                    | <p>Панель <i>красного</i> цвета отображается, если выполнены оба условия:</p> <ul style="list-style-type: none"> <li>• Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена.</li> <li>• Компонент Контроль запуска программ не установлен или задача запущена в режиме <b>Только статистика</b>.</li> </ul>                                                                                                                                                                                                                                                                                                             |
| <b>Лицензирование</b>              | <p>Панель <i>зеленого</i> цвета отображается при действующей лицензии.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                    | <p>Панель <i>желтого</i> цвета отображается, если возникло одно из следующих событий:</p> <ul style="list-style-type: none"> <li>• <i>Выполняется проверка статуса лицензии.</i></li> <li>• <i>До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации.</i></li> <li>• <i>Добавленный ключ помещен в черный список и будет заблокирован.</i></li> </ul>                                                                                                                                                                                                                                                   |

|            |                                                                                                                                                                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | Панель <i>красного</i> цвета отображается, если возникло одно из следующих событий: <ul style="list-style-type: none"> <li>• <i>Программа не активирована</i></li> <li>• <i>Срок действия лицензии истек</i></li> <li>• <i>Нарушено Лицензионное соглашение</i></li> <li>• <i>Ключ помещен в черный список</i></li> </ul> |
| Обновление | Панель <i>зеленого</i> цвета отображается, если базы программы актуальны.                                                                                                                                                                                                                                                 |
|            | Панель <i>желтого</i> цвета отображается, если базы программы устарели.                                                                                                                                                                                                                                                   |
|            | Панель <i>красного</i> цвета отображается, если базы программы сильно устарели.                                                                                                                                                                                                                                           |

## Просмотр статистики событий безопасности

На закладке **Статистика** отображаются все события безопасности. Статистика каждой задачи защиты отображается в отдельном блоке, где указано количество инцидентов, а также дата и время возникновения последнего инцидента. При регистрации инцидента цвет блока меняется на красный.

► Чтобы просмотреть статистику, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.  
Откроется **Диагностическое окно**.
3. Выберите закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

## Просмотр текущей активности программы

На этой закладке вы можете просматривать статус текущих задач и процессов программы, а также оперативно получать сообщения о происходящих критических событиях.

Для отображения статуса активности программы используется цветовая индикация:

- В разделе **Задачи**:
  - *Зеленый цвет*. Не выполнены условия, при которых требовалась бы индикация красным цветом.
  - *Желтый цвет*. Проверка важных областей не проводилась давно.
  - *Красный цвет*. Выполнено как минимум одно из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В разделе **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.



- **Желтый цвет.** Положение о KSN принято, но задача не запущена.
- Чтобы просмотреть текущую активность программы на защищаемом устройстве, выполните следующие действия:
1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
  2. Выберите пункт **Открыть Диагностическое окно.**  
Откроется **Диагностическое окно.**
  3. Выберите закладку **Текущая активность программы.**
  4. В разделе **Задачи** ознакомьтесь со следующей информацией:
    - **Проверка важных областей давно не выполнялась**
- Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
- **Выполняются сейчас**
  - **Завершены с ошибкой**
  - **Следующий запуск определен по расписанию**
5. В разделе **Kaspersky Security Network** ознакомьтесь со следующей информацией:
    - **Использование KSN включено. Включены запросы репутации файлов или Защита выключена**
    - **Использование KSN включено. Включены запросы репутации файлов, Статистика программы отправляется в KSN**
  6. В разделе **Интеграция с Kaspersky Security Center** ознакомьтесь со следующей информацией:
    - **Локальное управление разрешено**
    - **Применяется политика: <Имя Сервера администрирования>**

## Настройка записи файлов дампов и файлов трассировки

В диагностическом окне можно настроить запись файлов дампов и файлов трассировки.

Можно также настроить диагностику сбоев в Консоли программы (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. [153](#)).

- Чтобы запустить запись файлов дампов и файлов трассировки, выполните следующие действия:
1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
  2. Выберите пункт **Открыть Диагностическое окно.**

Откроется **Диагностическое окно**.

3. Выберите закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
  - a. Установите флажок **Записывать отладочную информацию в файл трассировки в данной папке**.
  - b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файлы трассировки.

Трассировка будет включена для всех компонентов с параметрами по умолчанию: с уровнем детализации *Отладка* и максимальным размером файла журнала – 50 МБ.

5. Если требуется, настройте следующие параметры записи файлов дампов:
  - a. Установите флажок **Создавать файл дампа по результатам сбоев в этой папке**.
  - b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Security для Windows Server будет сохранять файл дампа.

6. Нажмите на кнопку **Применить**.

Новая конфигурация будет применена.

# Обновление баз и модулей Kaspersky Security для Windows Server

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Security для Windows Server, копировании обновлений и откате обновлений баз Kaspersky Security для Windows Server, а также инструкции по настройке задач обновления баз и модулей программы.

## В этом разделе

|                                                                          |                     |
|--------------------------------------------------------------------------|---------------------|
| О задачах обновления .....                                               | <a href="#">211</a> |
| Об обновлении модулей программы .....                                    | <a href="#">212</a> |
| Об обновлении баз программы .....                                        | <a href="#">213</a> |
| Схемы обновления баз и модулей антивирусных программ в организации ..... | <a href="#">214</a> |
| Настройка задач обновления .....                                         | <a href="#">217</a> |
| Откат обновления баз Kaspersky Security для Windows Server .....         | <a href="#">224</a> |
| Откат обновления программных модулей .....                               | <a href="#">224</a> |
| Статистика задач обновления .....                                        | <a href="#">224</a> |

## О задачах обновления

В Kaspersky Security для Windows Server предусмотрено четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Security для Windows Server соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского" – каждый час. Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. [217](#)), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Security для Windows Server применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

### Обновление баз программы

По умолчанию Kaspersky Security для Windows Server копирует базы из источника обновлений на устройство и сразу переходит к их использованию в выполняющейся задаче Постоянная защита сервера. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление баз программы каждый час.

## Обновление модулей программы

По умолчанию Kaspersky Security для Windows Server проверяет доступность обновлений модулей программы в источнике обновлений. Для использования установленных программных модулей требуется перезагрузка защищаемого устройства и / или перезапуск Kaspersky Security для Windows Server.

По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Security для Windows Server, не копируя их.

Допускается устанавливать только обновления модулей программы, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу программы из сертифицированного состояния.

## Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Security для Windows Server загружает файлы обновлений баз программы и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

## Откат обновления баз программы

В ходе выполнения задачи Kaspersky Security для Windows Server возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

# Об обновлении модулей программы

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Security для Windows Server. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные (критичные) пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Security для Windows Server с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника, копируя на него обновления без установки, а затем распределяя их на защищаемые устройства в сети. Чтобы копировать и сохранять обновления без установки, используйте задачу Копирование обновлений.

Допускается устанавливать только обновления модулей программы, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу программы из сертифицированного состояния.

Перед установкой обновлений модулей, Kaspersky Security для Windows Server создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Security для Windows Server автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений.

На время установки полученных обновлений служба Kaspersky Security автоматически останавливается, а затем снова запускается.

## Об обновлении баз программы

Базы Kaspersky Security для Windows Server, хранящиеся на защищаемом устройстве, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз программы представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения устройства к минимуму, рекомендуется регулярно получать обновления баз программы.

По умолчанию, если базы Kaspersky Security для Windows Server не обновляются в течение недели с момента создания установленных обновлений баз, возникает событие *Базы программы устарели*. Если базы программы не обновляются в течение двух недель, возникает событие *Базы программы сильно устарели*. Информация об актуальности баз (см. раздел "Просмотр состояния защиты и информации о Kaspersky Security для Windows Server" на стр. [172](#)) отображается в панели результатов узла **Kaspersky Security** дерева Консоли программы. Вы можете использовать общие параметры Kaspersky Security для Windows Server, чтобы указать другое количество дней до возникновения этих событий. Вы можете также настроить уведомления администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. [269](#)).

Kaspersky Security для Windows Server загружает обновления баз и модулей программы с FTP- или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.

Можно загружать обновления на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника. На него будут копироваться обновления, а затем распространяться на защищаемые устройства. Если вы используете программу Kaspersky Security Center для централизованного управления защитой устройств в организации, можно использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз программы вручную или по расписанию (см. раздел "Настройка расписания запуска задач" на стр. [162](#)). По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление баз программы каждый час.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Security для Windows Server автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Security для Windows Server можно вручную откатить базы до ранее установленных обновлений (см. раздел "Откат обновлений баз Kaspersky Security для Windows Server" на стр. [224](#)).

## Схемы обновления баз и модулей антивирусных программ в организации

Выбор источника обновлений в задачах обновления зависит используемой в организации схемы обновления баз и модулей программы.

Вы можете обновлять базы и модули Kaspersky Security для Windows Server на защищаемых устройствах по следующим схемам:

- Загружать обновления напрямую из интернета на каждое защищаемое устройство (схема 1).
- Загружать обновления из интернета на устройство-посредник и распределять обновления на защищаемые устройства с этого устройства.

Посредником может служить любое устройство, на котором установлены следующие программы:

- Kaspersky Security для Windows Server (схема 2).
- Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через устройство-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность защищаемых устройств в сети.

Перечисленные схемы обновлений описаны ниже.

### Схема 1. Обновление баз и модулей программы напрямую из интернета

- Чтобы настроить получение обновлений Kaspersky Security для Windows Server напрямую из интернета,

на каждом защищаемом устройстве в параметрах задач Обновление баз программы и Обновление модулей программы укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.

Вы можете указать в качестве источников обновлений другие HTTP- или FTP-серверы, на которых имеется папка обновлений.

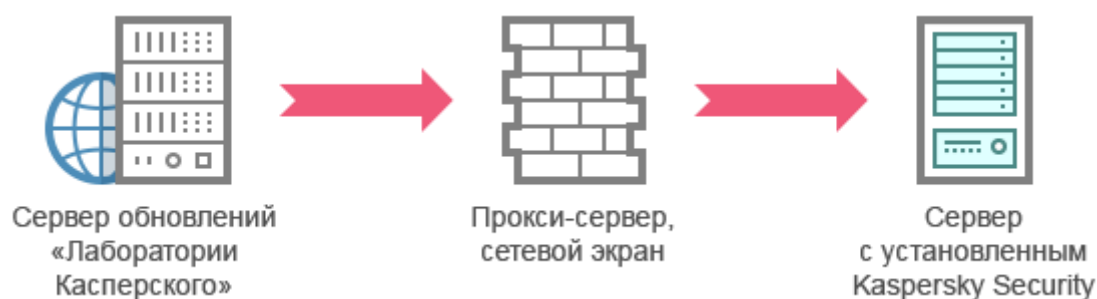


Рис. 1. Обновление баз и модулей программы напрямую из интернета

### Схема 2. Обновление баз и модулей программы через одно из защищаемых устройств

- Чтобы настроить получение обновлений Kaspersky Security для Windows Server через одно из защищаемых устройств, выполните следующие действия:

1. Скопируйте обновления на выбранное защищаемое устройство. Для этого выполните следующие действия:

- На выбранном защищаемом устройстве настройте параметры задачи Копирование обновлений:
  - а. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".
  - б. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.
- 2. Распределите обновления на остальные защищаемые устройства. Для этого выполните следующие действия:
  - На каждом защищаемом устройстве настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже).
    - а. В качестве источника обновлений укажите папку на диске устройства-посредника, в которую будут загружаться обновления.

Kaspersky Security для Windows Server будет получать обновления через одно из защищаемых устройств.

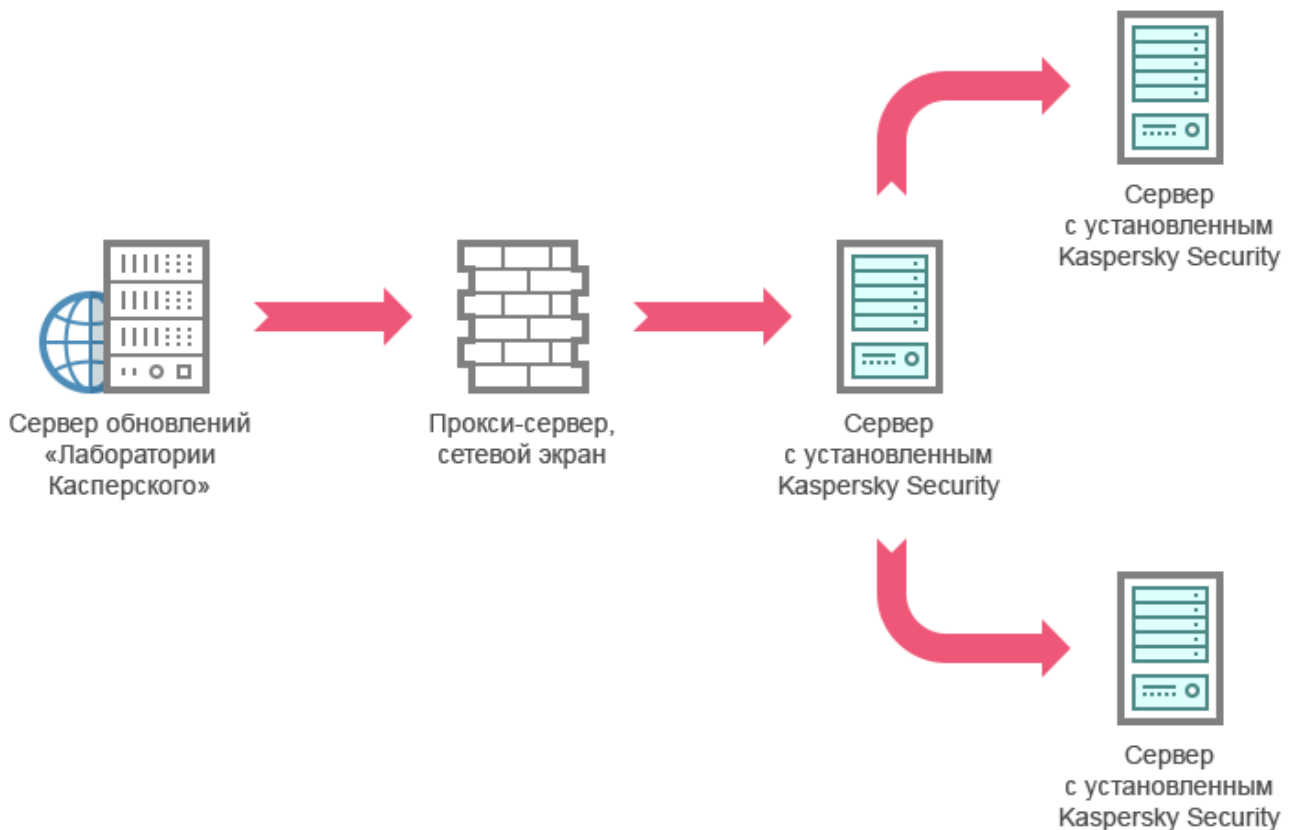


Рис. 2. Обновление баз и модулей программы через одно из защищаемых устройств

## Схема 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств, можно загружать обновления с помощью Сервера администрирования Kaspersky Security Center, установленного в локальной сети (см. рис. ниже).

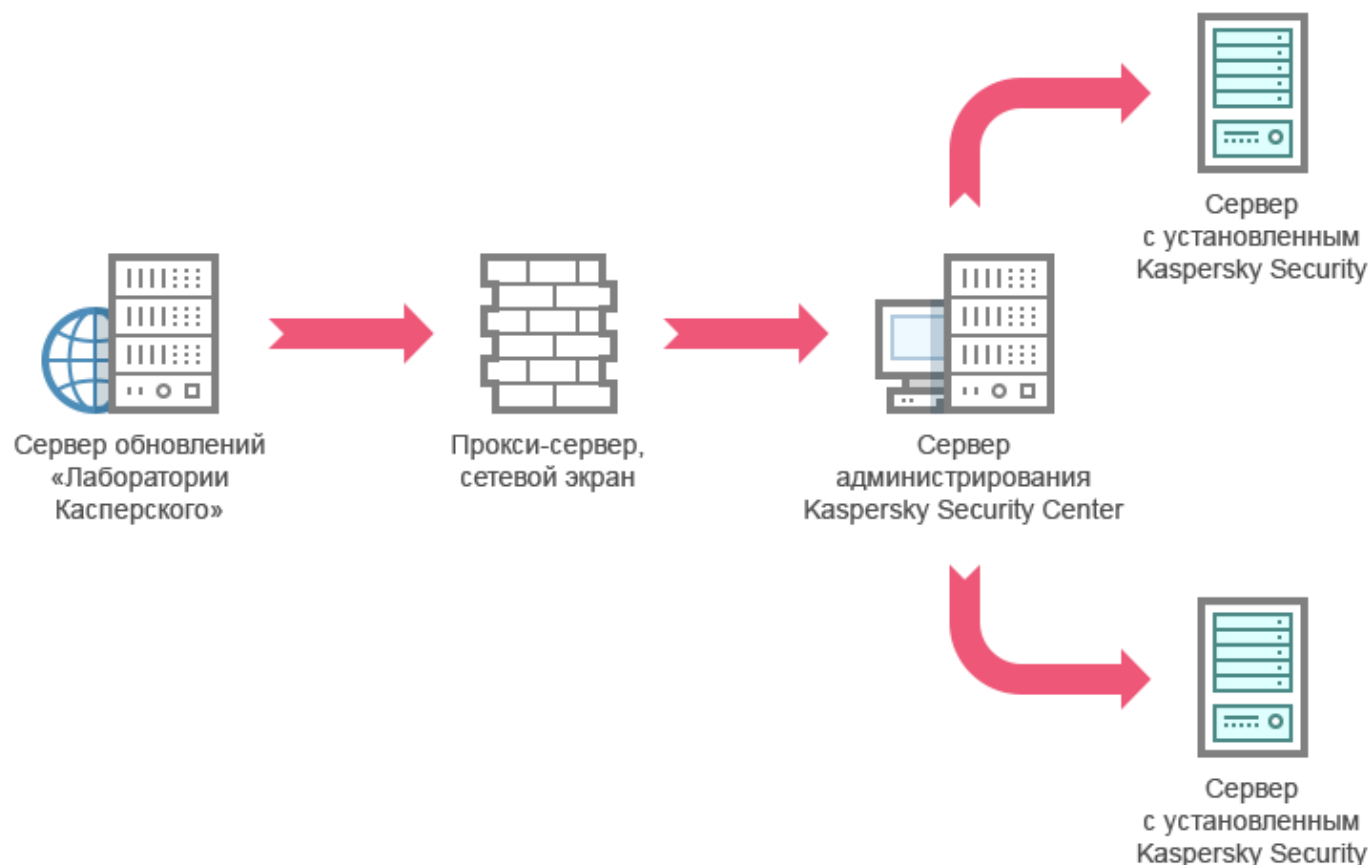


Рис. 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

► Чтобы настроить получение обновлений Kaspersky Security для Windows Server через Сервер администрирования Kaspersky Security Center, выполните следующие действия:

1. Загрузите обновления с серверов обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
  - Настройте задачу Получение обновлений Сервером администрирования для указанного набора защищаемых устройств:
    - а. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".
2. Распределите обновления на защищаемые устройства. Для этого выполните одно из следующих действий:
  - В Kaspersky Security Center настройте групповую задачу обновления антивирусных баз (модулей программы) для распределения обновлений на защищаемые устройства:
    - а. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.



Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

Частоту запуска **После получения обновлений Сервером администрирования** нельзя указать в Консоли программы.

- Настройте на каждом из защищаемых устройств задачи Обновление баз программы и Обновление модулей программы:
  - a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.
  - b. Если требуется, настройте расписание задачи.

При редких обновлениях антивирусных баз Kaspersky Security для Windows Server (от одного раза в месяц до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

Kaspersky Security для Windows Server будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых устройств Агент администрирования – программный компонент, входящий в комплект поставки Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Security для Windows Server на защищаемом устройстве. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

## Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Security для Windows Server.

### В этом разделе

|                                                                                                  |                     |
|--------------------------------------------------------------------------------------------------|---------------------|
| Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server ..... | <a href="#">217</a> |
| Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы .....             | <a href="#">220</a> |
| Настройка параметров задачи Копирование обновлений .....                                         | <a href="#">222</a> |
| Настройка параметров задачи Обновление модулей программы .....                                   | <a href="#">222</a> |

## Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, можно указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► Чтобы указать тип источника обновлений, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Источник обновлений** выберите тип источника обновлений Kaspersky Security для Windows Server:

- **Сервер администрирования Kaspersky Security Center**

Kaspersky Security для Windows Server использует Сервер администрирования Kaspersky Security Center в качестве источника обновления.

Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" осуществляется с помощью системы удаленного доступа Kaspersky Security Center и на защищаемом устройстве установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь защищаемых устройств с Сервером администрирования.

- **Серверы обновлений "Лаборатории Касперского"**

Kaspersky Security для Windows Server использует в качестве источников обновлений веб-сайты "Лаборатории Касперского". На этих веб-сайтах публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

Этот вариант выбран по умолчанию.

- **Другие HTTP-,FTP-серверы и сетевые ресурсы**

Kaspersky Security для Windows Server использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы или папки на серверах локальной сети.

Вы можете сформировать список источников, которые содержат актуальный набор обновлений, перейдя по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:
  - a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
    - i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.
    - ii. Нажмите на кнопку **ОК**.

- b. В разделе **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского"**, если указанные серверы недоступны.

Флажок включает или выключает функцию использования серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные вами источники обновлений недоступны.

Если флажок установлен, функция активна.

По умолчанию флажок установлен.

Вы можете установить флажок **Использовать серверы обновлений "Лаборатории Касперского"**, если указанные серверы недоступны, когда выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

- Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

Флажок включает или выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского" или если установлен флажок **Использовать серверы обновлений "Лаборатории Касперского"**, если указанные серверы недоступны.

Если флажок установлен, используются параметры прокси-сервера.

По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

Если флажок установлен, используются параметры прокси-сервера.

По умолчанию флажок снят.

Информация о настройке дополнительных параметров прокси-сервера и параметров аутентификации для доступа к прокси-серверу приведена в разделе **Запуск и настройка задачи Обновление баз программы**.

7. Нажмите на кнопку **ОК**.

Настроенные параметры источника обновлений Kaspersky Security для Windows Server будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Security для Windows Server.

- *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.

3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи** на закладке **Общие**.

4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

Откроется окно **Серверы обновлений**.

5. Выполните следующие действия:

- Чтобы добавить новый пользовательский источник обновления, нажмите на кнопку **Добавить** и в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере. Укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

По умолчанию добавленная папка используется в качестве источника обновлений.

- Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
- Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
- Чтобы изменить очередность обращения Kaspersky Security для Windows Server к пользовательским источникам обновлений, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, когда он должен использоваться: до или после других источников.
- Чтобы изменить путь к пользовательскому источнику обновлений, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
- Чтобы удалить пользовательский источник обновлений, выберите его в списке и нажмите на кнопку **Удалить**.

Вы не можете удалить единственный пользовательский источник из списка.

6. Нажмите на кнопку **ОК**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

## Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Security для Windows Server размещает файлы обновлений на локальном диске защищаемого устройства. Вы можете снизить нагрузку на дисковую подсистему защищаемого устройства за счет размещения файлов обновлений на виртуальном диске в оперативной памяти при выполнении задачи обновления.

Эта функция доступна для операционных систем Microsoft Windows Server 7 и выше.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

► Чтобы снизить нагрузку на дисковую подсистему защищаемого устройства при выполнении задачи Обновление баз программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Оптимизация использования дисковой подсистемы** настройте следующие параметры:

- Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

Флажок включает или выключает оптимизацию дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

Если флажок установлен, функция активна.

По умолчанию флажок снят.

- В поле **Объем оперативной памяти, используемый для оптимизации** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

- Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

## Настройка параметров задачи Копирование обновлений

► Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений**.
3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server" на стр. [217](#)).
5. На закладке **Общие** в разделе **Параметры копирования обновлений** выполните следующие действия:
  - Укажите условия копирования обновлений программы:
    - **Копировать обновления баз программы**  
Kaspersky Security для Windows Server загружает только обновления баз Kaspersky Security для Windows Server.  
Этот вариант выбран по умолчанию.
    - **Копировать критические обновления модулей программы**  
Kaspersky Security для Windows Server загружает только срочные обновления программных модулей Kaspersky Security для Windows Server.
    - **Копировать обновления баз программы и критические обновления модулей программы**  
Kaspersky Security для Windows Server загружает обновления баз и срочные обновления программных модулей Kaspersky Security для Windows Server.
  - Укажите локальную или сетевую папку, в которую Kaspersky Security для Windows Server будет копировать полученные обновления.
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

## Настройка параметров задачи Обновление модулей программы

► Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.

3. В панели результатов узла **Обновление модулей программы** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Security для Windows Server" на стр. [217](#)).
5. На закладке **Общие** в разделе **Параметры обновления** настройте параметры обновления модулей программы:
  - **Только проверять наличие доступных критических обновлений модулей программы**  
Kaspersky Security для Windows Server отображает уведомление об имеющихся срочных обновлениях программных модулей без загрузки обновлений.  
Уведомление отображается, если включено оповещение о событиях этого типа.  
Этот вариант выбран по умолчанию.
  - **Копировать и устанавливать критические обновления модулей программы**  
Kaspersky Security для Windows Server загружает и устанавливает критические обновления программных модулей.
  - **Разрешать перезагрузку операционной системы**  
Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.  
Если флажок установлен, Kaspersky Security для Windows Server выполняет перезагрузку операционной системы после установки обновлений, требующих перезагрузки.  
Флажок активен, если выбран вариант **Копировать и устанавливать критические обновления модулей программы**.  
По умолчанию флажок снят.
  - **Получать информацию о доступных плановых обновлениях модулей программы**  
Отображаются уведомления обо всех плановых обновлениях программных модулей Kaspersky Security для Windows Server, доступных в источнике обновлений. Программа отображает уведомление, если для данного типа событий включены уведомления.  
Если флажок установлен, отображается уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений.  
По умолчанию флажок установлен.
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)). По умолчанию Kaspersky Security для Windows Server запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете



настроить уведомление администратора о событии *Доступны новые критические и плановые обновления*, в котором будет содержаться адрес веб-страницы, откуда можно загрузить плановые обновления.

## Откат обновления баз Kaspersky Security для Windows Server

Перед применением обновления баз Kaspersky Security для Windows Server создает резервные копии баз, которые использовались ранее. Если обновление было прервано или завершилось с ошибкой, Kaspersky Security для Windows Server автоматически возвращается к использованию ранее установленных баз.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз программы.

► Чтобы запустить задачу *Откат обновления баз программы*,

в панели результатов узла **Откат обновления баз программы** перейдите по ссылке **Запустить**.

## Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Security для Windows Server создает резервные копии модулей, используемых в текущий момент. Если обновление модулей было прервано или завершилось с ошибкой, Kaspersky Security для Windows Server автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте функцию Microsoft Windows **Установка и удаление программ**.

## Статистика задач обновления

Во время выполнения задачи обновления вы можете просматривать актуальную информацию об объеме данных, загруженных с момента запуска задачи, а также прочую информацию о выполнении задачи.

После завершения или остановки задачи эту информацию можно просмотреть в журнале выполнения задачи.

► Чтобы просмотреть статистику задачи обновления, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.



В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Если вы просматриваете задачу Обновление баз программы или Копирование обновлений, в разделе **Статистика** отображается объем данных, загруженных Kaspersky Security для Windows Server на текущий момент (**Полученные данные**).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Table 45. Информация о задаче Обновление модулей программы

| Поле                                   | Описание                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Полученные данные</b>               | Общий объем полученных данных                                                                                                                                                                                                                                                                                             |
| <b>Доступно критических обновлений</b> | Количество критических обновлений, доступных для установки                                                                                                                                                                                                                                                                |
| <b>Доступно плановых обновлений</b>    | Количество плановых обновлений, доступных для установки                                                                                                                                                                                                                                                                   |
| <b>Ошибок применения обновлений</b>    | Если значение этого поля отличается от нуля, обновление не было применено. Название обновления, вызвавшего ошибку, можно посмотреть в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в журналах выполнения задач" на стр. <a href="#">251</a> ). |

# Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

## В этом разделе

|                                                                   |                     |
|-------------------------------------------------------------------|---------------------|
| Изолирование возможно зараженных объектов. Карантин .....         | <a href="#">226</a> |
| Резервное копирование объектов. Резервное хранилище .....         | <a href="#">236</a> |
| Блокировка доступа к сетевым ресурсам. Заблокированные узлы ..... | <a href="#">243</a> |

## Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

## В этом разделе

|                                                                                         |                     |
|-----------------------------------------------------------------------------------------|---------------------|
| Об изолировании возможно зараженных объектов.....                                       | <a href="#">226</a> |
| Просмотр объектов на карантине .....                                                    | <a href="#">227</a> |
| Проверка объектов на карантине .....                                                    | <a href="#">228</a> |
| Восстановление содержимого карантина.....                                               | <a href="#">230</a> |
| Помещение объектов на карантин .....                                                    | <a href="#">232</a> |
| Удаление объектов с карантина.....                                                      | <a href="#">232</a> |
| Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" ..... | <a href="#">233</a> |
| Настройка параметров карантина .....                                                    | <a href="#">234</a> |
| Статистика карантина.....                                                               | <a href="#">235</a> |

## Об изолировании возможно зараженных объектов

Kaspersky Security для Windows Server перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.

## Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов на карантине,*

отсортируйте объекты (см. раздел "Сортировка объектов на карантине" на стр. [227](#)) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. [227](#)).

### В этом разделе

|                                        |                     |
|----------------------------------------|---------------------|
| Сортировка объектов на карантине ..... | <a href="#">227</a> |
| Фильтрация объектов на карантине.....  | <a href="#">227</a> |

## Сортировка объектов на карантине

По умолчанию объекты на карантине отсортированы в таблице по дате помещения на карантин в обратном хронологическом порядке. Чтобы найти нужный объект, можно отсортировать объекты по графам с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок графы, по которой вы хотите отсортировать объекты в таблице.

Объекты в таблице писке будут отсортированы по выбранному параметру.

## Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, можно отфильтровать объекты в таблице – отобразить только те объекты, которые удовлетворяют заданным критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать фильтры, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.

2. Выберите вложенный узел **Карантин**.
3. В контекстном меню узла выберите пункт **Фильтр**.  
Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:
  - a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.
  - b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в таблице могут различаться в зависимости от значения, выбранного в списке **Название поля**.
  - c. В поле **Значение поля** введите или выберите в списке значение фильтра.
  - d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

- Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы изменить фильтр, выберите фильтр в списке в окне **Параметры фильтра**. Отредактируйте требуемые значения в полях **Имя поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.

5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► Чтобы вернуть отображение всех объектов на карантине,

в контекстном меню узла **Карантин** выберите пункт **Удалить фильтр**.

## Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Security для Windows Server выполняет системную задачу Проверка объектов на карантине. Параметры задачи приведены в следующей таблице. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Можно настроить расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)), используемой для запуска задачи.

Проверив объекты на карантине после обновления баз, Kaspersky Security для Windows Server может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Security для Windows Server может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Table 46. Параметры задачи Проверка объектов на карантине

| Параметр задачи Проверка объектов на карантине | Значение                                                                   |
|------------------------------------------------|----------------------------------------------------------------------------|
| Область проверки                               | Папка карантина                                                            |
| Параметры безопасности                         | Единые для всей области проверки (значения приводятся в следующей таблице) |

Table 47. Параметры безопасности в задаче Проверка объектов на карантине

| Параметр безопасности                                      | Значение                                                                                                                                                                                                    |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Проверка объектов                                          | Все объекты области проверки                                                                                                                                                                                |
| Оптимизация                                                | Выключено                                                                                                                                                                                                   |
| Действие над зараженными и другими обнаруженными объектами | Лечить, удалять, если лечение невозможно                                                                                                                                                                    |
| Действие над возможно зараженными объектами                | Пропускать                                                                                                                                                                                                  |
| Исключать объекты                                          | Нет                                                                                                                                                                                                         |
| Не обнаруживать                                            | Нет                                                                                                                                                                                                         |
| Останавливать проверку, если она длится более (сек.)       | Не задано                                                                                                                                                                                                   |
| Не проверять объекты размером более (МБ)                   | Не задано                                                                                                                                                                                                   |
| Альтернативные потоки NTFS                                 | Включена                                                                                                                                                                                                    |
| Загрузочные секторы дисков и MBR                           | Выключено                                                                                                                                                                                                   |
| Использовать технологию iChecker                           | Выключено                                                                                                                                                                                                   |
| Использовать технологию iSwift                             | Выключено                                                                                                                                                                                                   |
| Проверять составные объекты                                | <ul style="list-style-type: none"> <li>• Архивы*</li> <li>• SFX-архивы*</li> <li>• Упакованные объекты*</li> <li>• Вложенные OLE-объекты*</li> </ul> * Проверка только новых и измененных файлов выключена. |
| Проверка подписи Microsoft у файлов                        | Не выполняется                                                                                                                                                                                              |
| Использование эвристического                               | Включено с уровнем анализа <b>Глубокий</b>                                                                                                                                                                  |

| Параметр безопасности | Значение       |
|-----------------------|----------------|
| анализатора           |                |
| Доверенная зона       | Не применяется |

## Восстановление содержимого карантина

Kaspersky Security для Windows Server помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстановить любой объект с карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Security для Windows Server не изолировала этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать файлы** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в Доверенную зону (см. стр. [562](#)).

При восстановлении объектов можно выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом устройстве, в указанной папке на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению защищаемого устройства.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Security для Windows Server не включает его в составной объект при восстановлении. Объект, помещенный на карантин, сохраняется отдельно в выбранную папку.

Вы можете восстановить один или несколько объектов.

► Чтобы восстановить объекты с карантина, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выполните одно из следующих действий:
  - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.
  - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:
  - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
  - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
  - Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.
6. Чтобы сохранить копию объекта в папке *Карантин* после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.
7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.
  - a. Выберите одно из следующих действий Kaspersky Security для Windows Server:
    - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.

- **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
  - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.
- b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Заменить** или **Переименовать**, к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.
- c. Нажмите на кнопку **ОК**.
- Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.
- Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

## Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server поместит указанный файл на карантин.

## Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Security для Windows Server автоматически удаляет из папки карантина объекты, статус которых изменился на *Зараженный* при проверке карантина с использованием обновленных баз, если программа Kaspersky Security для Windows Server не смогла их вылечить. Kaspersky Security для Windows Server не удаляет остальные объекты из карантина.

Можно удалять объекты с карантина.

► *Чтобы удалить объекты с карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
  - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.



- Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.
- Выбранные объекты будут удалены с карантина.

## Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Security для Windows Server признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Security для Windows Server признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы с карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Нельзя отправлять объекты с карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

### ► Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:

1. Если файл не находится на карантине, предварительно поместите его на **Карантин**.
2. В узле **Карантин** откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.
3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.
4. Если на защищаемом устройстве, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

Поле **Получатель** содержит адрес электронной почты "Лаборатории Касперского" – [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com). Поле Тема содержит текст "Объект карантина".

Текст сообщения содержит следующую информацию: "Этот файл будет отправлен на анализ в Лабораторию Касперского". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

К сообщению будет приложен архив <имя объекта>.cab. Архив содержит файл <uuid>.klq с зашифрованным объектом, файл <uuid>.txt с информацией об объекте, полученной из Kaspersky Security для Windows Server, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Security для Windows Server и операционной системе защищаемого устройства:

- название и версию операционной системы;
- название и версию Kaspersky Security для Windows Server;
- дату выпуска последних установленных обновлений баз программы;
- активный ключ.

Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и более эффективно проанализировать файл. Однако если вы не хотите передавать эту информацию, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на защищаемом устройстве, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл можно переслать в "Лабораторию Касперского" самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **ОК**.
2. Выберите папку на диске защищаемого устройства или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

## Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

► *Чтобы настроить параметры карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства карантина** настройте нужные параметры карантина в соответствии с вашими требованиями:

- В разделе **Параметры карантина**:

- **Папка карантина**

Путь к папке карантина в формате UNC (Universal Naming Convention).

По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Quarantine\.

- **Максимальный размер карантина**

Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Security для Windows Server регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

Если флажок установлен, Kaspersky Security для Windows Server отслеживает суммарный размер размещенных в карантине объектов.

Если флажок снят, Kaspersky Security для Windows Server не отслеживает суммарный размер объектов в карантине.

По умолчанию флажок снят.

- **Порог доступного пространства**

Флажок включает или выключает отслеживание минимального объема свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Security для Windows Server регистрирует событие *Превышен порог свободного места в папке карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

Если флажок установлен, Kaspersky Security для Windows Server отслеживает размер свободного места в папке карантина.

Флажок **Порог доступного пространства (МБ)** активен, если установлен флажок **Максимальный размер карантина (МБ)**.

По умолчанию флажок установлен.

Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Security для Windows Server уведомит вас об этом, не переставая помещать объекты на карантин.

- В разделе **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**

Путь к папке, в которую восстанавливаются объекты, в формате UNC (Universal Naming Convention).

По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Restored\.

5. Нажмите на кнопку **ОК**.

Настроенные параметры карантина будут сохранены.

## Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы посмотреть статистику карантина,*

в дереве Консоли программы в контекстном меню узла **Карантин** выберите пункт **Статистика**.

В окне **Статистика карантина** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

| Поле                                | Описание                                                                                                                                                                  |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Возможно зараженных объектов</b> | Количество объектов, которые программа Kaspersky Security для Windows Server признала возможно зараженными.                                                               |
| <b>Текущий размер карантина</b>     | Общий объем данных в папке карантина.                                                                                                                                     |
| <b>Ложных срабатываний</b>          | Количество объектов, которым присвоен статус <i>Ложное срабатывание</i> , поскольку при проверке карантина с применением обновленных баз они были признаны незараженными. |
| <b>Вылечено объектов</b>            | Количество объектов, которым присвоен статус <i>Вылечен</i> после проверки карантина.                                                                                     |
| <b>Всего объектов</b>               | Общее количество объектов на карантине.                                                                                                                                   |

## Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

### В этом разделе

|                                                                     |                     |
|---------------------------------------------------------------------|---------------------|
| О резервном копировании объектов перед лечением или удалением ..... | <a href="#">236</a> |
| Просмотр объектов в резервном хранилище .....                       | <a href="#">237</a> |
| Восстановление файлов из резервного хранилища .....                 | <a href="#">239</a> |
| Удаление файлов из резервного хранилища .....                       | <a href="#">241</a> |
| Настройка параметров резервного хранилища .....                     | <a href="#">241</a> |
| Статистика резервного хранилища .....                               | <a href="#">242</a> |

## О резервном копировании объектов перед лечением или удалением

Kaspersky Security для Windows Server сохраняет зашифрованные копии объектов со статусом *зараженный* в папке *Резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Security для Windows Server сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Security для Windows Server признает зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Security для Windows Server помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Можно восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом устройстве или другом устройстве в локальной сети организации. Вы можете восстановить файл из резервного хранилища, если зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Security для Windows Server не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

## Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только с помощью узла **Резервное хранилище** Консоли программы. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► Чтобы просмотреть объекты в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► Чтобы найти нужный объект в списке объектов в резервном хранилище, отсортируйте объекты или отфильтруйте их.

### В этом разделе

|                                               |                     |
|-----------------------------------------------|---------------------|
| Сортировка файлов в резервном хранилище ..... | <a href="#">237</a> |
| Фильтрация файлов в резервном хранилище ..... | <a href="#">238</a> |

## Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их попадания в резервное хранилище в обратном хронологическом порядке. Чтобы найти нужный файл, отсортируйте файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В таблице файлов в узле **Резервное хранилище** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

## Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, можно отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

Откроется окно **Параметры фильтра**.

2. Чтобы добавить фильтр, выполните следующие действия:
  - a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.
  - b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут различаться в зависимости значения, выбранного в поле **Название поля**.
  - c. В поле **Значение поля** введите или выберите в списке значение фильтра.
  - d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

- Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.

После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

## Восстановление файлов из резервного хранилища

Kaspersky Security для Windows Server хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный зараженный файл содержал важную информацию и при лечении файла программа Kaspersky Security для Windows Server не смогла сохранить его целостность, в результате чего информация в файле стала недоступной;
- если вы считаете файл безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Security для Windows Server не признавала файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите файл в качестве значения параметра **Исключать файлы** или **Не обнаруживать** соответствующих задач.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходное местоположение (по умолчанию), в специальную папку для восстановленных объектов на защищаемом устройстве, в указанную папку на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. [241](#)).

По умолчанию, когда Kaspersky Security для Windows Server восстанавливает файл, его копия сохраняется в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:
  - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.
  - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.



Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:

- Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
- Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
- Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалять объекты из хранилища после восстановления** (по умолчанию флажок снят).

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

a. Выберите одно из следующих действий Kaspersky Security для Windows Server:

- **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
- **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
- **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Заменить** или **Переименовать**, к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

c. Нажмите на кнопку **ОК**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).



## Удаление файлов из резервного хранилища

► Чтобы удалить файлы из резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
  2. Выберите вложенный узел **Резервное хранилище**.
  3. Выполните одно из следующих действий:
    - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
    - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
  4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.
- Выбранные файлы будут удалены из резервного хранилища.

## Настройка параметров резервного хранилища

► Чтобы настроить параметры резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства резервного хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

В разделе **Параметры резервного хранилища**:

- **Папка резервного хранилища**

Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Backup\.

- **Максимальный размер резервного хранилища (МБ)**

Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Security для Windows Server регистрирует событие *Превышен максимальный размер резервного хранилища* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

Если флажок установлен, Kaspersky Security для Windows Server отслеживает суммарный размер размещенных в резервном хранилище объектов.

Если флажок снят, Kaspersky Security для Windows Server не отслеживает суммарный размер объектов в резервном хранилище.

По умолчанию флажок снят.

- **Порог доступного пространства (МБ)**

Флажок включает или выключает отслеживание минимального объема свободного

места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Security для Windows Server регистрирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

Если флажок установлен, Kaspersky Security для Windows Server отслеживает размер свободного места в резервном хранилище.

Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

По умолчанию флажок установлен.

Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Security для Windows Server уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В разделе **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**

Путь к папке, в которую восстанавливаются объекты, в формате UNC (Universal Naming Convention).

По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Restored\.

5. Нажмите на кнопку **ОК**.

Настроенные параметры резервного хранилища будут сохранены.

## Статистика резервного хранилища

Можно просматривать информацию о текущем состоянии резервного хранилища – статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

Table 48. Информация о текущем состоянии резервного хранилища

| Поле                                       | Описание                                                                                  |
|--------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Текущий размер резервного хранилища</b> | Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде |
| <b>Всего объектов</b>                      | Количество объектов в резервном хранилище в текущий момент                                |

## Блокировка доступа к сетевым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры хранилища заблокированных узлов.

### В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| О хранилище заблокированных узлов .....                    | <a href="#">243</a> |
| Включение блокировки недоверенных узлов .....              | <a href="#">244</a> |
| Настройка параметров хранилища заблокированных узлов ..... | <a href="#">245</a> |

## О хранилище заблокированных узлов

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов, Защита от шифрования для NetApp или Защита от шифрования. Эти компоненты обнаруживают попытки удаленных узлов зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных узлов. Информация о заблокированных узлах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа на защищаемом устройстве или к папкам сетевого хранилища для всех удаленных узлов из списка заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**.
- Для задачи Защита от шифрования: обнаружено вредоносное шифрование со стороны устройства, обращающегося к сетевым файловым ресурсам.
- Для задачи Защита от шифрования для NetApp: обнаружена атака на сетевое хранилище.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает событие *Предупреждение* для блокировки узла. Все попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локально уникальный идентификатор (LUID) атакующего узла добавлен в список заблокированных узлов, Kaspersky Security для Windows Server определяет IP-адрес этого узла и добавляет его в список заблокированных узлов вместо локально уникального идентификатора атакующего узла.

По умолчанию Kaspersky Security для Windows Server удаляет заблокированные узлы из списка через 30 минут после добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка заблокированных узлов. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

В случае запрета доступа к управлению хранилищами какому-либо пользователю, хранилище заблокированных узлов останется доступным. Параметры хранилища заблокированных узлов не могут быть изменены, если у пользователя отсутствует разрешение типа **Изменение прав** для управления Kaspersky Security для Windows Server.

## Включение блокировки недоверенных узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от шифрования
- Защита от шифрования для NetApp

► *Чтобы настроить задачу **Постоянная защита файлов**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**, если вы хотите, чтобы программа Kaspersky Security для Windows Server блокировала узлы, проявляющие вредоносную активность, во время выполнения задачи **Постоянная защита файлов**.
5. Если задача не была запущена, выберите закладку **Расписание**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу **Защита от шифрования**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладке **Общие** убедитесь, что задача запущена в режиме **Активный**.
5. Если задача не была запущена, выберите закладку **Расписание**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.

6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу **Защита от шифрования для NetApp**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита от шифрования для NetApp**.
3. В панели результатов перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладке **Общие** убедитесь, что задача запущена в режиме **Активный**.
5. Если задача не была запущена, выберите закладку **Расписание**:
  - a. Установите флажок **Запускать задачу по расписанию**.
  - b. В раскрывающемся списке выберите частоту запуска **При запуске задачи**.
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server блокирует доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность или попытки шифрования.

## Настройка параметров хранилища заблокированных узлов

► *Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
3. Выберите пункт меню **Свойства**.  
Откроется окно **Параметры хранилища заблокированных узлов**.
4. В разделе **Период блокировки узлов** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым ресурсам.
5. Нажмите на кнопку **ОК**.
6. Чтобы восстановить доступ для всех заблокированных узлов, выполните следующие действия:
  - a. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
  - b. Выберите пункт **Разблокировать все**.  
Все узлы будут удалены из списка и разблокированы.
7. Чтобы удалить узлы из списка заблокированных, выполните следующие действия:
  - a. В списке заблокированных узлов в панели результатов выберите один или несколько узлов.
  - b. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
  - c. Выберите пункт **Разблокировать выбранные**.  
Выбранные узлы будут разблокированы.

# Регистрация событий. Журналы Kaspersky Security для Windows Server

Этот раздел содержит информацию о работе с журналами Kaspersky Security для Windows Server: журналом системного аудита, журналами выполнения задач и журналом событий.

## В этом разделе

|                                                                                                  |                     |
|--------------------------------------------------------------------------------------------------|---------------------|
| Способы записи событий Kaspersky Security для Windows Server .....                               | <a href="#">246</a> |
| Журнал системного аудита .....                                                                   | <a href="#">247</a> |
| Журналы выполнения задач .....                                                                   | <a href="#">249</a> |
| Журнал безопасности .....                                                                        | <a href="#">253</a> |
| Просмотр журнала событий Kaspersky Security для Windows Server в оснастке Просмотр событий ..... | <a href="#">253</a> |
| Настройка параметров журналов с помощью Плагина управления .....                                 | <a href="#">254</a> |
| Настройка журналов и уведомлений .....                                                           | <a href="#">260</a> |

## Способы записи событий Kaspersky Security для Windows Server

События Kaspersky Security для Windows Server делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Security для Windows Server;
- события, связанные с управлением Kaspersky Security для Windows Server, например: запуск программы, создание или удаление задач, изменение параметров задач.

Kaspersky Security для Windows Server использует следующие способы записи событий:

- **Журналы выполнения задач.** Журнал выполнения задачи содержит информацию о текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита.** Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Security для Windows Server.
- **Журнал событий.** Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Security для Windows Server. Журнал событий доступен в "Просмотре событий" Microsoft Windows.
- **Журнал безопасности.** Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве.

Если в работе Kaspersky Security для Windows Server возникла проблема (например, Kaspersky Security для Windows Server или отдельная задача завершилась аварийно или не запустилась), то для ее диагностики можно создать файл трассировки и файл дампа памяти процессов Kaspersky Security для Windows Server и

отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Security для Windows Server не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Security для Windows Server. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

## Журнал системного аудита

Kaspersky Security для Windows Server ведет системный аудит событий, связанных с управлением Kaspersky Security для Windows Server. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Security для Windows Server, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли программы.

По умолчанию Kaspersky Security для Windows Server хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которую Kaspersky Security для Windows Server будет сохранять файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

### В этом разделе

|                                                      |                     |
|------------------------------------------------------|---------------------|
| Сортировка событий в журнале системного аудита ..... | <a href="#">247</a> |
| Фильтрация событий в журнале системного аудита ..... | <a href="#">248</a> |
| Удаление событий из журнала системного аудита .....  | <a href="#">249</a> |

## Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.



► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в таблице.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

## Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита записи только о тех событиях, которые удовлетворяют заданным условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

Откроется окно **Параметры фильтра**.

3. Чтобы добавить фильтр, выполните следующие действия:
  - a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать события.
  - b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
  - c. В списке **Значение поля** выберите значение фильтра.
  - d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:
  - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
  - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.



2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

В списке событий журнала системного аудита отобразятся все события.

## Удаление событий из журнала системного аудита

По умолчанию Kaspersky Security для Windows Server хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► Чтобы удалить события из журнала системного аудита, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.
3. Выполните одно из следующих действий:
  - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
  - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

## Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Security для Windows Server и инструкции по работе с ними.

### В этом разделе

|                                                                                                                   |                     |
|-------------------------------------------------------------------------------------------------------------------|---------------------|
| О журналах выполнения задач.....                                                                                  | <a href="#">250</a> |
| Сортировка журналов выполнения задач .....                                                                        | <a href="#">250</a> |
| Фильтрация журналов выполнения задач.....                                                                         | <a href="#">250</a> |
| Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в журналах выполнения задач..... | <a href="#">251</a> |
| Экспорт информации из журнала выполнения задачи .....                                                             | <a href="#">252</a> |
| Удаление журналов выполнения задач.....                                                                           | <a href="#">252</a> |

## О журналах выполнения задач

Информация о выполнении задач Kaspersky Security для Windows Server отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи можно просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи, а также параметры задачи.

По умолчанию Kaspersky Security для Windows Server хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Security для Windows Server сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Можно также выбрать события, записи о которых Kaspersky Security для Windows Server сохраняет в журналах выполнения задач.

## Сортировка журналов выполнения задач

По умолчанию журналу выполнения задач отображаются в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать журналы выполнения задач Kaspersky Security для Windows Server.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

## Фильтрация журналов выполнения задач

Вы можете настроить отображение в списке журналов выполнения задач только журналы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

► *Чтобы отфильтровать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.  
Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
  - a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать журналы выполнения задач.
  - b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
  - c. В списке **Значение поля** выберите значение фильтра.
  - d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:
  - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
  - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации в списке журналов выполнения задач.

В списке журналов выполнения задач отобразятся только журналы, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке журналов выполнения задач отобразятся все журналы.

## Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
  - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
  - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
4. В открывшемся окне отображается следующая информация:
  - На закладке **Статистика** отображается время запуска и завершения задачи и ее статистика.
  - На закладке **События** отображается список событий, зафиксированных во время выполнения задачи.
  - На закладке **Параметры** отображаются параметры задачи.
5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.

6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

7. Нажмите на кнопку **Заккрыть**.

Окно **Журналы** будет закрыто.

## Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
  - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
  - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
4. В нижней части окна **Журнал выполнения** нажмите на кнопку **Экспорт**.  
Откроется окно **Сохранить как**.
5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

## Удаление журналов выполнения задач

По умолчанию Kaspersky Security для Windows Server хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Можно вручную удалить журналы выполнения завершившихся задач.

События из журналов задач, выполняющихся в данный момент, и задач, используемых другими пользователями, удалены не будут.

► *Чтобы удалить журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:

- Чтобы удалить журналы выполнения всех завершившихся задач, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
  - Чтобы очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню журнала, который вы хотите очистить, и выберите пункт **Удалить**.
  - Чтобы очистить журналы выполнения нескольких задач, выполните следующие действия:
    - a. В панели результатов с помощью клавиш **CTRL** и **SHIFT** выберите журналы выполнения задач, которые вы хотите очистить.
    - b. Откройте контекстное меню любого журнала выполнения задач и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление журналов.
- Выбранные журналы выполнения задач будут очищены. Удаление журналов выполнения задач будет зарегистрировано в журнале системного аудита.

## Журнал безопасности

Kaspersky Security для Windows Server ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита сервера, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ).

Вы можете очистить журнал безопасности и журнал системного аудита (см. раздел "Удаление событий из журнала системного аудита" на стр. [249](#)). При очистке журнала безопасности Kaspersky Security для Windows Server регистрирует событие системного аудита.

## Просмотр журнала событий Kaspersky Security для Windows Server в оснастке Просмотр событий

С помощью оснастки Просмотр событий в Microsoft Management Console можно просматривать журнал событий Kaspersky Security для Windows Server. В журнале содержатся события, зарегистрированные Kaspersky Security для Windows Server и необходимые для диагностики сбоев в работе программы.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий;**
- **по уровню детализации.** Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются все события. Наименее подробным является уровень Критические события, при котором регистрируются только критические события.

- Чтобы просмотреть журнал событий Kaspersky Security для Windows Server, выполните следующие действия:
1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.  
Откроется Microsoft Management Console.
  2. Выберите **Файл > Добавить или удалить оснастку**.  
Откроется окно **Добавление и удаление оснасток**.
  3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.  
Откроется окно **Выбор компьютера**.
  4. В окне **Выбор компьютера** укажите защищаемое устройство, на котором установлена программа Kaspersky Security для Windows Server, и нажмите на кнопку **ОК**.
  5. В окне **Добавление и удаление оснасток** нажмите на кнопку **ОК**.  
В дереве Microsoft Management Console появится узел **Просмотр событий**.
  6. Раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб > Kaspersky Security**.  
Откроется журнал событий Kaspersky Security для Windows Server.

## Настройка параметров журналов с помощью Плагина управления

Вы можете настраивать следующие параметры журналов Kaspersky Security для Windows Server:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
  - местоположение папки, в которой Kaspersky Security для Windows Server сохраняет файлы журналов выполнения задач и журнала системного аудита;
  - пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*;
  - события, которые Kaspersky Security для Windows Server сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Security для Windows Server в оснастке **Просмотр событий**;
  - параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.
- Чтобы настроить параметры журналов Kaspersky Security для Windows Server, выполните следующие действия:
1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.  
Откроется окно **Параметры журналов и уведомлений**.
  2. В окне **Параметры журналов и уведомлений** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

- На закладке **Общие**, если требуется, выберите события, которые Kaspersky Security для Windows Server сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Security для Windows Server в оснастке Просмотр событий. Для этого выполните следующие действия:
  - В списке **Компонент** выберите компонент Kaspersky Security для Windows Server, уровень детализации событий которого вы хотите указать.

Для компонентов Постоянная защита файлов, Защита RPC-подключаемых сетевых хранилищ, Защита ICAP-подключаемых сетевых хранилищ, Проверка скриптов, Проверка по требованию и Обновление предусмотрена запись событий в журналы выполнения задач и в журнал событий. Для этих компонентов таблица событий содержит графы **Журнал выполнения задачи** и **Журнал событий Windows**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица событий содержит графы **Аудит** и **Журнал событий Windows**.

- В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.  
 В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.
- Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:
  - a. В списке **Уровень важности** выберите **Другой**.
  - b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.
- На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий для состояния защиты устройства:
  - В разделе **Хранение журналов**:
    - **Папка журналов**  
 Путь к папке с журналами в формате UNC (Universal Naming Convention).  
 По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Reports\.  
 Если используемый по умолчанию путь изменился, создается папка с соответствующим именем. Новые файлы журналов будут сохранены в новую папку. Созданные ранее файлы журналов останутся в старой папке.
    - **Удалять журналы выполнения задач старше чем (дни)**  
 Флажок включает или выключает функцию, которая удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).  
 Если флажок установлен, Kaspersky Security для Windows Server удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени.



По умолчанию флажок установлен.

- **Удалять из журнала системного аудита события старше чем (дни)**

Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

Если флажок установлен, Kaspersky Security для Windows Server удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

По умолчанию флажок снят.

- В разделе **Пороги формирования событий**:

- Укажите количество дней, по истечении которого будут регистрироваться события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*.

Table 49. Пороги формирования событий

| Параметр              | Пороги формирования событий.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Описание              | Вы можете указать пороги формирования событий следующих типов:<br><i>Базы программы устарели</i> и <i>Базы программы сильно устарели</i> . События возникают, если базы Kaspersky Security для Windows Server не обновляются в течение указанного параметром количества дней с момента выпуска последних установленных обновлений баз. Вы можете настроить уведомление администратора об этих событиях.<br><i>Проверка важных областей давно не выполнялась</i> . Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком <b>Считать выполнение задачи проверкой важных областей</b> . |
| Возможные значения    | Количество дней от 1 до 365.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Значение по умолчанию | Базы программы устарели – 7 дней.<br>Базы программы сильно устарели – 14 дней.<br>Проверка важных областей давно не выполнялась – 30 дней.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере (см. раздел "Настройка параметров интеграции с SIEM" на стр. [257](#)).

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

## В этом разделе

|                                              |                     |
|----------------------------------------------|---------------------|
| Об интеграции с SIEM .....                   | <a href="#">257</a> |
| Настройка параметров интеграции с SIEM ..... | <a href="#">257</a> |



## Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Security для Windows Server может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

### Параметры надежности

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удастся подключиться к основному syslog-серверу или использовать его.

Также Kaspersky Security для Windows Server использует события системного аудита для уведомления о неудачных попытках подключения к SIEM-серверу и об ошибках отправки событий на SIEM-сервер.

## Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Table 50. Параметры интеграции с SIEM

| Параметр                                                                          | Значение по умолчанию            | Описание                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Отправлять события по протоколу syslog на внешний syslog-сервер                   | Не применяется                   | Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.                                                                                                        |
| Удалять локальные копии событий при записи на внешний syslog-сервер               | Не применяется                   | Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок.                                                                 |
| Формат событий                                                                    | Структурированные данные         | Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.                      |
| Протокол подключения                                                              | TCP                              | Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UDP или TCP с помощью выпадающего списка.                                                          |
| Параметры подключения к основному syslog-серверу                                  | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.       |
| Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен | Не применяется                   | Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.                                                                                                         |
| Параметры подключения к дополнительному syslog-серверу                            | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4. |

► Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры журналов и уведомлений**.
3. Выберите закладку **Интеграция с SIEM**.
4. В разделе **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

Если флажок установлен, программа выполняет отправку публикуемых событий на SIEM-сервер в соответствии с настроенными параметрами интеграции с SIEM.

Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

По умолчанию флажок снят.

5. Если требуется, в разделе **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

Флажок включает или выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

6. В разделе **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В разделе **Параметры соединения**:

- Укажите протокол подключения к SIEM.
- Укажите параметры соединения с основным syslog-сервером.  
IP-адрес можно указать только в формате IPv4.
- Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.

Укажите следующие параметры подключения к дополнительному syslog-серверу: **Адрес** и **Порт**.

Поля **Адрес** и **Порт** для дополнительного syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

IP-адрес можно указать только в формате IPv4.

8. Нажмите на кнопку **ОК**.

Настроенные параметры интеграции с SIEM будут применены.

## Настройка журналов и уведомлений

В Консоли администрирования Kaspersky Security Center можно настроить уведомление администратора и пользователей о следующих событиях, связанных с работой Kaspersky Security для Windows Server и состоянием антивирусной защиты устройства:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому устройству, и пользователи терминального защищаемого устройства могут получать информацию о событиях *Обнаружен объект*.

Можно настроить уведомления о событиях Kaspersky Security для Windows Server как для отдельного защищаемого устройства в окне **Свойства: <Имя защищаемого устройства>** выбранного защищаемого устройства, так и для группы защищаемых устройств в окне **Свойства: <Имя политики>** выбранной группы администрирования.

На закладке **Уведомления о событиях** или в окне **Параметры уведомлений** можно настроить следующие типы уведомлений:

- На закладке **Уведомления о событиях** (стандартная закладка в Kaspersky Security Center) можно настроить уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений содержится в *Справке Kaspersky Security Center*.
- В окне **Параметры уведомлений** можно настроить уведомления как администратора, так и пользователей.

Уведомления о событиях некоторых типов можно настраивать только на закладке или только в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите уведомления о событиях одного типа в одинаковом режиме на закладке **Уведомления о событиях** и в окне **Параметры уведомлений**, системный администратор будет получать уведомления об этих событиях дважды.

### В этом разделе

|                                                                 |                     |
|-----------------------------------------------------------------|---------------------|
| Настройка параметров журналов .....                             | <a href="#">261</a> |
| Журнал безопасности .....                                       | <a href="#">262</a> |
| Настройка параметров интеграции с SIEM .....                    | <a href="#">262</a> |
| Настройка параметров уведомлений .....                          | <a href="#">265</a> |
| Настройка обмена информацией с Сервером администрирования ..... | <a href="#">266</a> |

## Настройка параметров журналов

► Чтобы настроить параметры журналов Kaspersky Security для Windows Server, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Журналы выполнения задач** нажмите на кнопку **Настройка**.
5. В окне **Параметры журналов** настройте следующие параметры Kaspersky Security для Windows Server согласно вашим требованиям:
  - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
    - a. В списке **Компонент** выберите компонент Kaspersky Security для Windows Server, уровень детализации событий которого вы хотите указать.
    - b. Чтобы задать уровень детализации в журналах выполнения задач и в журнале системного аудита для выбранного компонента, выберите требуемый уровень в списке **Уровень важности**.
  - Чтобы изменить расположение журналов по умолчанию, укажите полный путь к папке или выберите папку с помощью кнопки **Обзор**.
  - Укажите, сколько дней будут храниться журналы выполнения задач.
  - Укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита**.
6. Нажмите на кнопку **ОК**.

Настроенные параметры журналов будут сохранены.

## Журнал безопасности

Kaspersky Security для Windows Server ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита сервера, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ).

Вы можете очистить журнал безопасности и журнал системного аудита (см. раздел "Удаление событий из журнала системного аудита" на стр. [249](#)). При очистке журнала безопасности Kaspersky Security для Windows Server регистрирует событие системного аудита.

## Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.  
Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.
- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

**Программа никогда не удаляет локальные версии журнала безопасности.**

Kaspersky Security для Windows Server может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удастся подключиться к основному syslog-серверу или использовать его.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Table 51. Параметры интеграции с SIEM

| Параметр                                                                                 | Значение по умолчанию            | Описание                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Отправлять события по протоколу syslog на внешний syslog-сервер</b>                   | Не применяется                   | Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.                                                                                                           |
| <b>Удалять локальные копии событий при записи на внешний syslog-сервер</b>               | Не применяется                   | Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок.                                                                    |
| Формат событий                                                                           | Структурированные данные         | Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.                         |
| Протокол подключения                                                                     | TCP                              | С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам UDP или TCP, к дополнительному syslog-серверу по протоколу TCP.                             |
| Параметры подключения к основному syslog-серверу                                         | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4.       |
| <b>Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен</b> | Не применяется                   | Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.                                                                                                            |
| Параметры подключения к дополнительному syslog-серверу                                   | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4. |

► Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:



- Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Журналы выполнения задач** нажмите на кнопку **Настройка**.  
Откроется окно **Параметры журналов и уведомлений**.
5. Выберите закладку **Интеграция с SIEM**.
6. В разделе **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

Если флажок установлен, программа выполняет отправку публикуемых событий на SIEM-сервер в соответствии с настроенными параметрами интеграции с SIEM.

Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

По умолчанию флажок снят.

7. Если требуется, в разделе **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

Флажок включает или выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

8. В разделе **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

По умолчанию программа выполняет конвертацию в формат структурированных данных.

9. В разделе **Параметры соединения**:



- Укажите протокол подключения к SIEM.
- Укажите параметры соединения с основным syslog-сервером.  
IP-адрес можно указать только в формате IPv4.
- Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.

Укажите следующие параметры подключения к дополнительному syslog-серверу: **Адрес** и **Порт**.

Поля **Адрес** и **Порт** для дополнительного syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

IP-адрес можно указать только в формате IPv4.

10. Нажмите на кнопку **ОК**.

Настроенные параметры интеграции с SIEM будут применены.

## Настройка параметров уведомлений

► Чтобы настроить уведомления Kaspersky Security для Windows Server, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Уведомления о событиях** нажмите на кнопку **Настройка**.
5. В окне **Параметры уведомлений** настройте следующие параметры Kaspersky Security для Windows Server согласно вашим требованиям:
  - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.

- В разделе **Уведомление пользователей** настройте способ уведомления пользователей. Если требуется, задайте текст уведомления.
- В разделе **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
- В разделе **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Security для Windows Server регистрирует события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*.
  - **Базы программы устарели (сут)**  
Количество дней с момента последнего обновления баз программы.  
По умолчанию установлено 7 дней.
  - **Базы программы сильно устарели (сут)**  
Количество дней с момента последнего обновления баз программы.  
По умолчанию установлено 14 дней.
  - **Проверка важных областей давно не выполнялась (сут)**  
Количество дней с момента последнего успешного завершения задачи Проверка важных областей.  
По умолчанию установлено 30 дней.

6. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

## Настройка обмена информацией с Сервером администрирования

- Чтобы выбрать типы объектов, информацию о которых Kaspersky Security для Windows Server будет передавать на Сервер администрирования Kaspersky Security Center, выполните следующие действия:
1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой требуется настроить параметры программы.
  3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
    - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел **"Настройка политики"** на стр. [124](#)).
    - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел **"Настройка локальных задач в окне Параметры программы в Kaspersky Security Center"** на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.



4. В разделе **Журналы и уведомления** в подразделе **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.

Откроется окно **Сетевые списки Сервера администрирования**.

5. В окне **Сетевые списки Сервера администрирования** выберите типы объектов, информацию о которых Kaspersky Security для Windows Server будет передавать на Сервер администрирования Kaspersky Security Center:
  - объекты на карантине;
  - резервные копии объектов;
  - заблокированные узлы.
6. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server будет передавать информацию о выбранных типах объектов на Сервер администрирования.

# Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Security для Windows Server о событиях программы и состоянии защиты устройства, а также инструкцию по настройке уведомлений.

## В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| Способы уведомления администратора и пользователей .....   | <a href="#">268</a> |
| Настройка уведомлений администратора и пользователей ..... | <a href="#">269</a> |

## Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к устройству, о событиях, связанных с работой Kaspersky Security для Windows Server, и о состоянии антивирусной защиты устройства.

Программа обеспечивает выполнение следующих задач:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к устройству, и пользователи терминального устройства могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли программы можно активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  - a. Средства службы терминалов.  
Вы можете применять этот способ для оповещения пользователей терминального защищаемого устройства, если защищаемое устройство является терминальным.
  - b. Средства службы сообщений.  
Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows. Этот способ неприменим, если защищаемое устройство работает под управлением операционной системы Microsoft Windows Server 2008 или выше.
- Способы уведомления администраторов:
  - a. Средства службы сообщений.  
Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows. Этот способ неприменим, если защищаемое устройство работает под управлением операционной системы Microsoft Windows Server 2008 или выше.
  - b. Запуск исполняемого файла.  
При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого устройства.

- с. Отправка по электронной почте.

Этот способ использует для передачи сообщений электронную почту.

Вы можете составить текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

## Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► Чтобы настроить уведомления о событиях, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** выберите способ уведомления:
  - а. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.
  - б. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

Уведомление пользователя можно настроить только для следующих событий: **Обнаружен объект, Обнаружено и заблокировано недоверенное запоминающее устройство и Недоверенный узел в списке**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:
  - а. Нажмите на кнопку **Текст сообщения**.
  - б. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

Вы можете составить один текст сообщения для нескольких типов событий: после выбора способа уведомлений для одного типа событий, выберите остальные типы событий, для которых вы хотите использовать этот же текст сообщения, с помощью клавиш **CTRL** и **SHIFT**, а затем нажмите на кнопку **Текст сообщения**.

- с. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.
- д. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.
4. Чтобы настроить способы уведомления администраторов о выбранном событии, выберите закладку **Уведомления** и в разделе **Уведомление администраторов** нажмите на кнопку **Настройка**. Затем в окне **Дополнительные параметры** выполните настройку выбранных способов уведомления. Для этого выполните следующие действия:

- a. Для уведомлений по электронной почте выберите закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса точкой с запятой), имя или сетевой адрес SMTP-сервера и номер порта. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** можно также добавлять переменные с информацией о событии (см. таблицу ниже).

Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

- b. Для уведомлений средствами службы сообщений Windows составьте список защищаемых устройств, получающих уведомления, на закладке **Служба сообщений Windows**: для каждого защищаемого устройства, которое вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

Уведомления службы сообщений Windows не используются, если защищаемое устройство работает под управлением операционной системы Microsoft Windows Server 2008 или более поздних версий Microsoft Windows Server.

- c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите файл на локальном диске защищаемого устройства или введите полный путь к нему. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Если вы хотите ограничить количество уведомлений о событиях одного типа за период времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите количество экземпляров и период времени.

5. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

Table 52. Поля с информацией о событии

| Переменная       | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %EVENT_TYPE%     | Тип события.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| %EVENT_TIME%     | Время возникновения события.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| %EVENT_SEVERITY% | Уровень важности события.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %OBJECT%         | Имя объекта (в задачах постоянной защиты сервера и проверки по требованию).<br>В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.                                                                                                                                                                                                                                                                                                                                                                                  |
| %VIRUS_NAME%     | Имя объекта согласно классификации Вирусной энциклопедии <a href="https://encyclopedia.kaspersky.ru/knowledge/classification/">https://encyclopedia.kaspersky.ru/knowledge/classification/</a> . Это имя входит в полное название обнаруженного объекта, которое Kaspersky Security для Windows Server возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в журналах выполнения задач" на стр. <a href="#">251</a> ). |
| %VIRUS_TYPE%     | Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Security для Windows Server возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.                                                                                                                                                                                                                     |
| %USER_COMPUTER%  | В задачах Постоянная защита файлов и Защита RPC-подключаемых сетевых хранилищ – имя защищаемого устройства пользователя, который обратился к объекту на устройстве.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| %USER_NAME%      | В задачах Постоянная защита файлов и Защита RPC-подключаемых сетевых хранилищ – имя пользователя, который обратился к объекту на устройстве.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| %FROM_COMPUTER%  | Имя защищаемого устройства, с которого поступило уведомление.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| %EVENT_REASON%   | Причина возникновения события (некоторые события не имеют этого поля).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| %ERROR_CODE%     | Код ошибки (только для события "внутренняя ошибка задачи").                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| %TASK_NAME%      | Название задачи (имеется только у событий, связанных с выполнением задач).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Запуск и остановка Kaspersky Security для Windows Server

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security.

## В этом разделе

|                                                                                                                    |                     |
|--------------------------------------------------------------------------------------------------------------------|---------------------|
| Запуск Плагина управления Kaspersky Security для Windows Server .....                                              | <a href="#">272</a> |
| Запуск Консоли Kaspersky Security для Windows Server из меню Пуск .....                                            | <a href="#">272</a> |
| Запуск и остановка службы Kaspersky Security .....                                                                 | <a href="#">273</a> |
| Запуск компонентов Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы ..... | <a href="#">274</a> |

## Запуск Плагина управления Kaspersky Security для Windows Server

Для запуска Плагина управления Kaspersky Security для Windows Server в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на защищаемое устройство администратора, он запускается вместе с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

## Запуск Консоли Kaspersky Security для Windows Server из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► Чтобы запустить Консоль программы из меню **Пуск**, выполните следующие действия:

1. В меню **Пуск** выберите **Программы > Kaspersky Security для Windows Server > Средства администрирования > Консоль Kaspersky Security для Windows Server**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:

1. В меню **Пуск** выберите **Программы > Kaspersky Security для Windows Server > Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.



Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом устройстве откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом устройстве, подключитесь к защищаемому устройству.

► *Чтобы подключиться к защищаемому устройству, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите команду **Подключиться к другому компьютеру**.  
Откроется окно **Выбор компьютера**.
3. В открывшемся окне выберите **Другой компьютер**.
4. В поле ввода справа укажите сетевое имя защищаемого устройства.
5. Нажмите на кнопку **ОК**.

Консоль программы подключится к защищаемому устройству.

Если учетная запись, используемая для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на защищаемом устройстве, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

## Запуск и остановка службы Kaspersky Security

По умолчанию служба Kaspersky Security запускается автоматически сразу после операционной системы. Служба Kaspersky Security управляет рабочими процессами, в которых выполняются задачи постоянной защиты сервера, контроля сервера, проверки по требованию и обновления.

По умолчанию при запуске Kaspersky Security для Windows Server запускаются задачи Постоянная защита файлов, Проверка скриптов (если установлена) и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security, программа автоматически запустит только задачи, в расписании которых указано **При запуске программы**. Остальные задачи нужно запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security с помощью контекстного меню узла **Kaspersky Security** или с помощью оснастки Службы Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Security для Windows Server, если вы входите в группу администраторов на защищаемом устройстве.

► *Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите одну из следующих команд:
  - **Остановить службу**

- **Запустить службу**

Служба Kaspersky Security будет запущена или остановлена.

## Запуск компонентов Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы

В этом разделе приведена информация о работе Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы.

### В этом разделе

|                                                                                                         |                     |
|---------------------------------------------------------------------------------------------------------|---------------------|
| О работе Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы..... | <a href="#">274</a> |
| Запуск Kaspersky Security для Windows Server в безопасном режиме .....                                  | <a href="#">275</a> |

## О работе Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы

Компоненты Kaspersky Security для Windows Server можно запустить при загрузке операционной системы в безопасном режиме. Наряду со службой Kaspersky Security (kavfs.exe) загружается драйвер klam.sys. Драйвер используется для регистрации службы Kaspersky Security как защищенной службы при загрузке операционной системы. Дополнительные сведения приведены в разделе "Регистрация службы Kaspersky Security как защищенной службы".

Kaspersky Security для Windows Server можно запустить при загрузке операционной системы в следующих безопасных режимах:

- Безопасный режим с типом загрузки "Минимальная" – стандартный вариант безопасного режима загрузки операционной системы. При этом Kaspersky Security для Windows Server может запускать следующие компоненты:
  - Постоянная защита файлов.
  - Проверка по требованию.
  - Контроль запуска программ и Формирование правил контроля запуска программ.
  - Анализ журналов.
  - Мониторинг файловых операций.
  - Мониторинг целостности файлов на основе эталона.
  - Проверка целостности программы.
  - Защита от шифрования.
  - Хранилище заблокированных узлов.

Безопасный режим с типом загрузки "Сеть" – загрузка операционной системы в безопасном режиме с поддержкой сетевых драйверов. В этом режиме помимо компонентов, запускаемых в безопасном режиме с типом загрузки "Минимальная", Kaspersky Security для Windows Server может запускать следующие компоненты:

- Обновление баз программы.
- Обновление модулей программы.
- Защита сетевых хранилищ.

## Запуск Kaspersky Security для Windows Server в безопасном режиме

По умолчанию Kaspersky Security для Windows Server не запускается при загрузке операционной системы в безопасном режиме.

► *Чтобы запустить Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение 1.
5. Нажмите на кнопку **ОК**.

► *Чтобы отменить запуск Kaspersky Security для Windows Server при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение 0.
5. Нажмите на кнопку **ОК**.

# Механизмы самозащиты Kaspersky Security для Windows Server

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Security для Windows Server.

## В этом разделе

|                                                                                                     |                     |
|-----------------------------------------------------------------------------------------------------|---------------------|
| О механизмах самозащиты Kaspersky Security для Windows Server .....                                 | <a href="#">276</a> |
| Защита от изменений папок с установленными компонентами Kaspersky Security для Windows Server ..... | <a href="#">276</a> |
| Защита от изменений ключей реестра Kaspersky Security для Windows Server .....                      | <a href="#">276</a> |
| Регистрация службы Kaspersky Security как защищенной службы .....                                   | <a href="#">277</a> |
| Управление правами доступа к функциям Kaspersky Security для Windows Server .....                   | <a href="#">278</a> |

## О механизмах самозащиты Kaspersky Security для Windows Server

В Kaspersky Security для Windows Server реализованы механизмы самозащиты, обеспечивающие защиту от изменения или удаления папок программы, процессов памяти и записей системного реестра.

### Защита от изменений папок с установленными компонентами Kaspersky Security для Windows Server

Kaspersky Security для Windows Server запрещает всем пользователям переименовывать и удалять папки с установленными компонентами программы. По умолчанию используются следующие пути к папкам установки программы:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security для Windows Server\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\

### Защита от изменений ключей реестра Kaspersky Security для Windows Server

Kaspersky Security для Windows Server ограничивает доступ к следующим ключам и ветвям реестра, обеспечивающим загрузку драйверов и служб программы:

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE]

- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klelam]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\11\CrashDump]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\CrashDump] (в 64-разрядной версии Microsoft Windows)
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\11\Trace]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\11\Trace] (в 64-разрядной версии Microsoft Windows)

Права на изменение этих ветвей и ключей реестра имеют только пользователи с учетной записью Локальная система (SYSTEM). Пользователи с учетными записями Пользователь и Администратор имеют права только на чтение.

## Регистрация службы Kaspersky Security как защищенной службы

Технология *Protected Process Light* (PPL) гарантирует, что операционная система выполняет загрузку только доверенных служб и процессов. Для того чтобы запустить службу как защищенную, на устройстве должен быть установлен драйвер *Early Launch Antimalware*.

Драйвер *Early Launch Antimalware* (далее "драйвер ELAM") обеспечивает защиту устройств в сети при их включении и при инициализации драйверов сторонних производителей.

Драйвер ELAM устанавливается автоматически во время установки Kaspersky Security для Windows Server и используется для регистрации службы Kaspersky Security как защищенной во время запуска операционной системы. Когда служба Kaspersky Security (KAVFS) запускается как системный защищенный процесс, другие незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищенного процесса и останавливать службу.

При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM возможна в операционной системе Microsoft Windows Server 2016 и более поздних версий. Если программа Kaspersky Security для Windows Server установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

- Чтобы установить Kaspersky Security как защищенный процесс, выполните следующую команду:

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

## Управление правами доступа к функциям Kaspersky Security для Windows Server

Этот раздел содержит информацию о правах на управление Kaspersky Security для Windows Server и службами операционной системы, которые регистрирует программа, а также инструкции по настройке этих прав.

### В этом разделе

|                                                                    |                     |
|--------------------------------------------------------------------|---------------------|
| О правах на управление Kaspersky Security для Windows Server ..... | <a href="#">278</a> |
| О правах на управление регистрируемыми службами .....              | <a href="#">280</a> |
| О правах доступа к службе Kaspersky Security Management .....      | <a href="#">281</a> |
| О правах на управление службой Kaspersky Security .....            | <a href="#">281</a> |
| Управление правами доступа с помощью Плагина управления .....      | <a href="#">283</a> |
| Управление правами доступа с помощью Консоли программы .....       | <a href="#">287</a> |
| Управление правами доступа с помощью Веб-плагина.....              | <a href="#">290</a> |

## О правах на управление Kaspersky Security для Windows Server

По умолчанию доступ ко всем функциям Kaspersky Security для Windows Server имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, пользователи группы KAVWSEE Administrators, созданной на защищаемом устройстве при установке Kaspersky Security для Windows Server, а также группа SYSTEM.

Пользователи, которые имеют доступ уровня Изменение прав в Kaspersky Security для Windows Server, могут предоставлять доступ к функциям Kaspersky Security для Windows Server другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Security для Windows Server, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа:

- **Полный контроль** — доступ ко всем функциям программы: возможность просматривать и изменять общие параметры Kaspersky Security для Windows Server, параметры компонентов и права пользователей Kaspersky Security для Windows Server, а также возможность просматривать статистику Kaspersky Security для Windows Server.

- **Изменение** – доступ ко всем функциям программы, за исключением изменения прав пользователей: возможность просматривать и изменять общие параметры Kaspersky Security для Windows Server и параметры компонентов Kaspersky Security для Windows Server.
- **Чтение** – возможность просматривать общие параметры Kaspersky Security для Windows Server, параметры компонентов Kaspersky Security для Windows Server, статистику Kaspersky Security для Windows Server и права пользователей Kaspersky Security для Windows Server.

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Security для Windows Server.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Table 53. Права доступа к функциям Kaspersky Security для Windows Server

| Права доступа                                    | Описание                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Управление задачами                              | Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Security для Windows Server.                                                                                                                                                                                                                                             |
| Создание и удаление задач проверки по требованию | Возможность создавать и удалять задачи проверки по требованию.                                                                                                                                                                                                                                                                                                    |
| Изменение параметров                             | Возможности: <ul style="list-style-type: none"> <li>• Импортировать в конфигурационный файл параметры работы Kaspersky Security для Windows Server.</li> <li>• Редактировать настройки программы.</li> </ul>                                                                                                                                                      |
| Чтение параметров                                | Возможности: <ul style="list-style-type: none"> <li>• Просматривать общие параметры Kaspersky Security для Windows Server и параметры задач.</li> <li>• Экспортировать параметры Kaspersky Security для Windows Server в конфигурационный файл.</li> <li>• Просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.</li> </ul> |
| Управление хранилищами                           | Возможности: <ul style="list-style-type: none"> <li>• Помещать объекты на карантин.</li> <li>• Удалять объекты из карантина и резервного хранилища.</li> <li>• Восстанавливать объекты из карантина и резервного хранилища.</li> </ul>                                                                                                                            |
| Управление журналами                             | Возможность удалять журналы выполнения задач и очищать журнал системного аудита.                                                                                                                                                                                                                                                                                  |
| Чтение журналов                                  | Возможность просматривать события в журналах выполнения задач и журнале системного аудита.                                                                                                                                                                                                                                                                        |
| Чтение статистики                                | Возможность просматривать статистику работы каждой задачи Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                  |
| Лицензирование программы                         | Возможность активировать Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                   |
| Удаление программы                               | Возможность удалить Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                        |
| Чтение прав                                      | Возможность просматривать список и права доступа пользователей Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                             |



| Права доступа  | Описание                                                                                                                                                                                                                                     |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Изменение прав | <p>Возможности:</p> <ul style="list-style-type: none"> <li>Изменять список пользователей, имеющих доступ к управлению программой.</li> <li>Изменять права доступа пользователей к функциям Kaspersky Security для Windows Server.</li> </ul> |

## О правах на управление регистрируемыми службами

При установке Kaspersky Security для Windows Server регистрирует в Windows службу Kaspersky Security (KAVFS), службу Kaspersky Security Management (KAVFSGT) и службу Kaspersky Security Exploit Prevention (KAVFSSLP).

Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Если программа Kaspersky Security для Windows Server установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

### Служба Kaspersky Security

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Пользователи, имеющие доступ уровня Изменение прав (см. раздел "Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля" на стр. [289](#)), могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

### Служба Kaspersky Security Management

Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Security для Windows Server, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, и пользователи группы KAVWSEE Administrators, созданной на защищаемом устройстве при установке Kaspersky Security для Windows Server.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

### Служба Kaspersky Security Exploit Prevention

По умолчанию доступ к управлению службой Kaspersky Security Exploit Prevention имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также в группу SYSTEM с правами на чтение и исполнение.



## О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Security для Windows Server.

При установке Kaspersky Security для Windows Server регистрирует службу Kaspersky Security Management (KAVFSGT). Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, используемая для подключения к Kaspersky Security для Windows Server, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, и пользователи группы KAVWSEE Administrators, созданной на защищаемом устройстве при установке Kaspersky Security для Windows Server.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Нельзя разрешить или запретить пользователям доступ к службе Kaspersky Security Management при настройке параметров Kaspersky Security для Windows Server.

Вы можете подключиться к Kaspersky Security для Windows Server с локальной учетной записью, если на защищаемом устройстве зарегистрирована учетная запись с таким же именем пользователя и паролем.

## О правах на управление службой Kaspersky Security

При установке Kaspersky Security для Windows Server регистрирует в Windows службу Kaspersky Security (KAVFS), так как программа включает в себя функциональные компоненты, запускаемые при старте операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности защищаемого устройства через управление службой Kaspersky Security, вы можете ограничить права на управление службой Kaspersky Security с помощью Консоли программы или Плагина управления.

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Нельзя удалить или изменять права для учетной записи SYSTEM. Если права учетной записи SYSTEM были изменены, при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ уровня Изменение прав к функциям (см. раздел "О правах на управление Kaspersky Security для Windows Server" на стр. 278), могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security для Windows Server один из следующих стандартных уровней доступа для управления службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security, а также запускать и останавливать службу Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security.
- **Исполнение** – возможность запускать и останавливать службу Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Security для Windows Server (см. таблицу ниже).

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Table 54. Разграничение прав доступа к функциям Kaspersky Security для Windows Server

| Функция                                                | Описание                                                                                                                                     |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Просмотр параметров службы                             | Возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.                                               |
| Запрос статуса службы у Диспетчера управления службами | Возможность запрашивать статус выполнения службы Kaspersky Security у Диспетчера управления службами Microsoft Windows.                      |
| Запрос статуса у службы                                | Возможность запрашивать статус службы у службы Kaspersky Security.                                                                           |
| Перечисление зависимых служб                           | Возможность просматривать список служб, от которых зависит служба Kaspersky Security, а также служб, зависимых от службы Kaspersky Security. |
| Изменение параметров службы                            | Возможность просматривать и изменять общие параметры работы и права пользователей для служб Kaspersky Security.                              |
| Запуск службы                                          | Возможность запускать выполнение службы Kaspersky Security.                                                                                  |
| Остановка службы                                       | Возможность останавливать выполнение службы Kaspersky Security.                                                                              |
| Приостановка / Возобновление службы                    | Возможность приостанавливать и возобновлять выполнение службы Kaspersky Security.                                                            |
| Чтение прав                                            | Возможность просматривать список пользователей службы Kaspersky Security и права доступа каждого пользователя.                               |

| Функция                           | Описание                                                                                                                                                                                                   |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Изменение прав                    | Возможности: <ul style="list-style-type: none"> <li>• добавлять и удалять пользователей службы Kaspersky Security;</li> <li>• изменять права доступа пользователей к службе Kaspersky Security.</li> </ul> |
| Удаление службы                   | Возможность отмены регистрации службы Kaspersky Security в диспетчере управления службами Microsoft Windows.                                                                                               |
| Пользовательские запросы к службе | Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.                                                                                                                   |

## Управление правами доступа с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка прав доступа для одного или всех защищаемых устройств сети.

### В этом разделе

Настройка прав доступа к Kaspersky Security для Windows Server и службе Kaspersky Security .... [283](#)

Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля ..... [286](#)

## Настройка прав доступа к Kaspersky Security для Windows Server и службе Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Security для Windows Server и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

► Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительно** выполните одно из следующих действий:

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

Откроется окно **Разрешения для Kaspersky Security для Windows Server**.

5. В открывшемся окне выполните следующие действия:

- Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
- Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► Чтобы изменить права пользователя или группы на управление Kaspersky Security для Windows Server или службой Kaspersky Security, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительно** выполните одно из следующих действий:

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
  - Нажмите на кнопку **Настройка** в подразделе **Права пользователей не управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.
- Откроется окно **Разрешения для Kaspersky Security**.
5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
  6. В блоке **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
    - **Полный контроль**: полный набор прав на управление Kaspersky Security для Windows Server или службой Kaspersky Security.
    - **Чтение**:
      - Следующие разрешения на управление Kaspersky Security для Windows Server: **Получение статистики, Чтение параметров, Чтение журналов, Чтение прав.**
      - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы, Запрос статуса службы у Диспетчера управления службами, Запрос статуса у службы, Перечисление зависимых служб, Чтение прав.**
    - **Изменение**:
      - Все права на управление Kaspersky Security для Windows Server, кроме **Изменение прав.**
      - Следующие права на управление службой Kaspersky Security: **Изменение параметров службы, Чтение прав.**
    - **Особые разрешения**: следующие разрешения на управление службой Kaspersky Security: **Запуск службы, Остановка службы, Остановка / возобновление службы, Чтение прав, Пользовательские запросы к службе.**
  7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
    - a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Security** выберите нужного пользователя или группу.
    - b. Нажмите на кнопку **Изменить**.
    - c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.
    - d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.
    - e. Нажмите на кнопку **ОК**.
    - f. В окне **Дополнительные параметры безопасности для службы Kaspersky Security** нажмите на кнопку **ОК**.
  8. В окне **Разрешения для службы Kaspersky Security** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Security для Windows Server или службой Kaspersky Security будут сохранены.

## Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Security для Windows Server.

Kaspersky Security для Windows Server запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Security для Windows Server;
- изменение компонентов Kaspersky Security для Windows Server;
- выполнение команд командной строки.

Интерфейс Kaspersky Security для Windows Server скрывает вводимый пароль на экране. Kaspersky Security для Windows Server хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Security для Windows Server не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара (\$), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► Чтобы защитить доступ к функциям Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Выберите группу администрирования, содержащую защищаемые устройства, для которых вы хотите настроить параметры программы.

2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры политики для группы защищаемых устройств, выберите закладку **Политики** и с помощью контекстного меню перейдите к свойствам **<Имя политики>**.
  - Если вы хотите настроить параметры программы для отдельного защищаемого устройства, откройте окно **Параметры программы** в Kaspersky Security Center (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).
3. На закладке **Параметры программы** в разделе **Безопасность** нажмите на кнопку **Настройка**.  
Откроется окно **Параметры безопасности**.
4. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.  
Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Security для Windows Server.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Security для Windows Server будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

## Управление правами доступа с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка прав доступа для защищаемого устройства.

### В этом разделе

|                                                                                                               |                     |
|---------------------------------------------------------------------------------------------------------------|---------------------|
| Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security ..... | <a href="#">287</a> |
| Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля .....                        | <a href="#">289</a> |

## Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Security для Windows Server и управлению службой Kaspersky Security, а также изменять права доступа этих пользователей и групп пользователей.



► *Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security** и выполните одно из следующих действий:
  - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
  - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению службой Kaspersky Security.

Откроется окно **Разрешения для Kaspersky Security**.

2. В открывшемся окне выполните следующие действия:
  - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу.
  - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу и нажмите на кнопку **Удалить**.

3. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Security для Windows Server или службой Kaspersky Security, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security** и выполните одно из следующих действий:
  - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите настроить права доступа к функциям Kaspersky Security для Windows Server.
  - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите настроить права доступа к службе Kaspersky Security.

Откроется окно **Разрешения для Kaspersky Security**.

2. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
3. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
  - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
  - Нажмите на кнопку **Настройка** в подразделе **Права пользователей не управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

Откроется окно **Разрешения для Kaspersky Security**.

4. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.



5. В блоке **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
  - **Полный контроль:** полный набор прав на управление Kaspersky Security для Windows Server или службой Kaspersky Security.
  - **Чтение:**
    - Следующие разрешения на управление Kaspersky Security для Windows Server: **Получение статистики, Чтение параметров, Чтение журналов, Чтение прав.**
    - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы, Запрос статуса службы у Диспетчера управления службами, Запрос статуса у службы, Перечисление зависимых служб, Чтение прав.**
  - **Изменение:**
    - Все права на управление Kaspersky Security для Windows Server, кроме **Изменение прав.**
    - Следующие права на управление службой Kaspersky Security: **Изменение параметров службы, Чтение прав.**
  - **Особые разрешения:** следующие разрешения на управление службой Kaspersky Security: **Запуск службы, Остановка службы, Остановка / возобновление службы, Чтение прав, Пользовательские запросы к службе.**
6. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
  - a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Security** выберите нужного пользователя или группу.
  - b. Нажмите на кнопку **Изменить**.
  - c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.
  - d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.
  - e. Нажмите на кнопку **ОК**.
  - f. В окне **Дополнительные параметры безопасности для службы Kaspersky Security** нажмите на кнопку **ОК**.
7. В окне **Разрешения для службы Kaspersky Security** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Security для Windows Server или службой Kaspersky Security будут сохранены.

## Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Security для Windows Server.

Kaspersky Security для Windows Server запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;

- удаление Kaspersky Security для Windows Server;
- изменение компонентов Kaspersky Security для Windows Server;
- выполнение команд командной строки.

Интерфейс Kaspersky Security для Windows Server скрывает вводимый пароль на экране. Kaspersky Security для Windows Server хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► Чтобы защитить доступ к функциям Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Security** и выполните одно из следующих действий:
  - В панели результатов узла перейдите по ссылке **Свойства программы**.
  - В контекстном меню узла выберите пункт **Свойства**.Откроется окно **Параметры программы**.
2. На закладке **Безопасность и надежность** в разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.  
Поля **Пароль** и **Подтверждение пароля** станут активными.
3. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Security для Windows Server.
4. В поле **Подтверждение пароля** введите пароль повторно.
5. Нажмите на кнопку **ОК**.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

## Управление правами доступа с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка прав доступа для защищаемых устройств сети.

## В этом разделе

|                                                                                                 |                     |
|-------------------------------------------------------------------------------------------------|---------------------|
| Настройка прав доступа к Kaspersky Security для Windows Server и службе Kaspersky Security .... | <a href="#">291</a> |
| Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля .....          | <a href="#">291</a> |

## Настройка прав доступа к Kaspersky Security для Windows Server и службе Kaspersky Security

Чтобы настроить права доступа для пользователя или группы, необходимо указать строку дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL). Дополнительная информация о строке дескриптора безопасности приведена на веб-сайте Microsoft.

► *Чтобы настроить права доступа для пользователя или группы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Выполните одно из следующих действий:
  - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Security для Windows Server.
  - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.
6. Добавьте пользователя или группу, указав строку дескриптора безопасности в окне **Права пользователей на управление программой** или **Права пользователей на управление службой Kaspersky Security**.
7. Нажмите на кнопку **ОК**.

## Защита доступа к функциям Kaspersky Security для Windows Server с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Security для Windows Server.

Kaspersky Security для Windows Server запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Security для Windows Server;
- изменение компонентов Kaspersky Security для Windows Server;
- выполнение команд командной строки.

Интерфейс Kaspersky Security для Windows Server скрывает вводимый пароль на экране. Kaspersky Security для Windows Server хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► Чтобы защитить доступ к функциям Kaspersky Security для Windows Server, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. В разделе **Безопасность** нажмите на кнопку **Настройка**.
6. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.
7. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Security для Windows Server.
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Security для Windows Server будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

# Постоянная защита файлов

Этот раздел содержит информацию о задаче Постоянная защита файлов и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

|                                                                                     |                     |
|-------------------------------------------------------------------------------------|---------------------|
| О задаче Постоянная защита файлов .....                                             | <a href="#">293</a> |
| Об области защиты и параметрах безопасности задачи.....                             | <a href="#">294</a> |
| О виртуальной области защиты .....                                                  | <a href="#">295</a> |
| Стандартные области защиты.....                                                     | <a href="#">295</a> |
| Стандартные уровни безопасности .....                                               | <a href="#">296</a> |
| Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов ..... | <a href="#">298</a> |
| Параметры задачи Постоянная защита файлов по умолчанию .....                        | <a href="#">300</a> |
| Управление задачей Постоянная защита файлов с помощью Плагина управления.....       | <a href="#">302</a> |
| Управление задачей Постоянная защита файлов с помощью Консоли программы .....       | <a href="#">317</a> |
| Управление задачей Постоянная защита файлов с помощью Веб-плагина .....             | <a href="#">338</a> |

## О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Security для Windows Server проверяет следующие объекты защищаемого устройства при доступе к ним:

- файлы;
- альтернативные потоки данных NTFS;
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;
- файлы-контейнеры Windows Server 2016 и Windows Server 2019.

При записи или считывании файла любой программой на защищаемом устройстве, Kaspersky Security для Windows Server перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Перед лечением или удалением Kaspersky Security для Windows Server сохраняет зашифрованную копию исходного файла в папку резервного хранилища.

Kaspersky Security для Windows Server перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016 и Windows Server 2019.

*Контейнер* – это изолированная среда, где программа может работать без прямого взаимодействия с операционной системой. Если контейнер расположен в области защиты задачи, Kaspersky Security для Windows Server проверяет файлы контейнера, к которому получают доступ пользователи, на наличие компьютерных угроз. При обнаружении угрозы, программа пытается вылечить контейнер. Если лечение успешно, контейнер продолжает работу. Если лечение невозможно, контейнер выключается.

Kaspersky Security для Windows Server также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих параметрах.

## Об области защиты и параметрах безопасности задачи

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы устройства. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов устройства, контролируемых Kaspersky Security для Windows Server. По умолчанию сетевые файловые ресурсы устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

- *Чтобы перейти к отображению сетевых файловых ресурсов в виде дерева в Консоли программы,*

в раскрывающемся списке в левом верхнем углу окна **Параметры области защиты** выберите элемент **Показывать в виде дерева**.

Независимо от того, отображаются ли файловые ресурсы защищаемого устройства в виде списка или в виде дерева, значки узлов имеют следующие значения:

 – узел включен в область защиты.

 – узел исключен из области защиты.

 – по крайней мере один из узлов, вложенных в этот узел, исключен из области защиты, или параметры безопасности вложенных узлов отличаются от параметров безопасности родительского узла (только при отображении в виде дерева).

Значок  отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области защиты для выбранного вложенного узла.

С помощью Консоли программы можно также добавлять в область защиты виртуальные диски (см. раздел "Формирование виртуальной области защиты" на стр. [327](#)). Имена виртуальных узлов отображаются синим цветом.

### Параметры безопасности

Можно настроить как единые параметры безопасности задачи для всех узлов или элементов, входящих в область защиты, так и различные для всех узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. [296](#));
- настроить параметры безопасности вручную (см. раздел "Настройка параметров безопасности вручную" на стр. [310](#)) для выбранных узлов или элементов в дереве или списке файловых ресурсов (уровень безопасности примет значение **Пользовательский**).

Вы можете сохранить набор параметров узла или элемента в шаблон, чтобы потом применять этот шаблон для других узлов или элементов.

## О виртуальной области защиты

Kaspersky Security для Windows Server может проверять не только существующие папки и файлы на жестких и съемных дисках, но и диски, временно подключенные к защищаемому устройству, например, общие диски кластера, которые динамически создаются на защищаемом устройстве различными программами и службами.

Если все объекты устройства включены в область защиты, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для динамических узлов или если вы выбрали для защиты отдельные области устройства, то, для того чтобы включить в область защиты виртуальные диски, файлы или папки, вам нужно предварительно создать их в Консоли программы, то есть задать виртуальную область защиты. Созданные диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого устройства.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, все появившиеся в ней виртуальные папки или файлы не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

## Стандартные области защиты

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Security для Windows Server предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски.** Kaspersky Security для Windows Server защищает файлы на жестких дисках устройства.
- **Съемные диски.** Kaspersky Security для Windows Server защищает файлы на внешних устройствах, например, на компакт-дисках или флеш-накопителях. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.



- **Сетевое окружение.** Kaspersky Security для Windows Server защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на устройстве. Kaspersky Security для Windows Server не защищает файлы, когда к ним обращаются программы с других защищаемых устройств.
- **Виртуальные диски.** Можно включать в область защиты виртуальные папки и файлы, а также диски, временно подключенные к устройству, например, общие диски кластера.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

По умолчанию в область защиты включены все стандартные области, кроме виртуальных дисков.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы включить в область защиты объекты на виртуальном диске, включите в область защиты папку на устройстве, связанную с этим виртуальным диском.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов защищаемого устройства. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

## Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

### Максимальное быстроедействие

Уровень безопасности **Максимальное быстроедействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Security для Windows Server на защищаемых устройствах и рабочих станциях, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

### Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

### Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности устройств в сети организации.



Table 55. Стандартные уровни безопасности и соответствующие им значения параметров

| Параметры                                                                                                                        | Уровень безопасности                                                                               |                                                                                                                                                         |                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                  | Максимальное<br>быстродействие                                                                     | Рекомендуемый                                                                                                                                           | Максимальная<br>защита                                                                                                                    |
| <b>Защита объектов</b>                                                                                                           | По расширению                                                                                      | По формату                                                                                                                                              | По формату                                                                                                                                |
| <b>Проверка только новых и измененных файлов</b>                                                                                 | Включена                                                                                           | Включена                                                                                                                                                | Выключено                                                                                                                                 |
| <b>Действия над зараженными и другими обнаруженными объектами</b>                                                                | Блокировать доступ и лечить.<br>Удалить, если не удалось вылечить.                                 | Блокировать доступ и лечить.<br>Удалить, если не удалось вылечить.                                                                                      | Блокировать доступ и лечить.<br>Удалить, если не удалось вылечить.                                                                        |
| <b>Действия над возможно зараженными объектами</b>                                                                               | Блокировать доступ и поместить на карантин.                                                        | Блокировать доступ и поместить на карантин.                                                                                                             | Блокировать доступ и поместить на карантин.                                                                                               |
| <b>Исключать файлы</b>                                                                                                           | Нет                                                                                                | Нет                                                                                                                                                     | Нет                                                                                                                                       |
| <b>Не обнаруживать</b>                                                                                                           | Нет                                                                                                | Нет                                                                                                                                                     | Нет                                                                                                                                       |
| <b>Останавливать проверку, если она длится более (сек)</b>                                                                       | 60 сек.                                                                                            | 60 сек.                                                                                                                                                 | 60 сек.                                                                                                                                   |
| <b>Не проверять составные объекты размером более (МБ)</b>                                                                        | 8 МБ                                                                                               | 8 МБ                                                                                                                                                    | Не установлен                                                                                                                             |
| <b>Альтернативные потоки NTFS</b>                                                                                                | Да                                                                                                 | Да                                                                                                                                                      | Да                                                                                                                                        |
| <b>Проверять загрузочные секторы дисков и MBR</b>                                                                                | Да                                                                                                 | Да                                                                                                                                                      | Да                                                                                                                                        |
| <b>Защита составных объектов</b>                                                                                                 | <ul style="list-style-type: none"> <li>Упакованные объекты*</li> </ul> * Только новые и измененные | <ul style="list-style-type: none"> <li>SFX-архивы*</li> <li>Упакованные объекты*</li> <li>Вложенные OLE-объекты*</li> </ul> * Только новые и измененные | <ul style="list-style-type: none"> <li>SFX-архивы*</li> <li>Упакованные объекты*</li> <li>Вложенные OLE-объекты*</li> </ul> * Все объекты |
| <b>Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой</b> | Нет                                                                                                | Нет                                                                                                                                                     | Да                                                                                                                                        |

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** и **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените параметры безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** или **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

## Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Security для Windows Server проверяет файлы, имеющие следующие расширения:

- 386;
- acm;
- ade, adp;
- asp;
- asx;
- ax;
- bas;
- bat;
- bin;
- chm;
- cla, clas\*;
- cmd;
- com;
- cpl;
- crt;
- dll;
- dpl;
- drv;
- dvb;
- dwg;
- efi;
- emf;
- eml;
- exe;
- fon;
- fpm;
- hlp;
- hta;
- htm, html\*;

- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm\*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*

- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm\*;*
- *swf;*
- *sys;*
- *the;*
- *them\*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

## Параметры задачи Постоянная защита файлов по умолчанию

По умолчанию в задаче Постоянная защита файлов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 56. Параметры задачи Постоянная защита файлов по умолчанию

| Параметр                                                                                  | Значение по умолчанию                                                                    | Описание                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Область защиты                                                                            | Защищаемое устройство целиком, исключая виртуальные диски.                               | Вы можете изменить область защиты.                                                                                                                                                                                                                                                                                                                                                                        |
| Параметры безопасности                                                                    | Единые для всей области защиты; соответствует уровню безопасности <b>Рекомендуемый</b> . | Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: <ul style="list-style-type: none"> <li>• выбрать другой стандартный уровень безопасности;</li> <li>• вручную изменить параметры безопасности.</li> </ul> Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла. |
| Режим защиты объектов                                                                     | При открытии и изменении                                                                 | Вы можете выбрать режим защиты – указать, при каком типе доступа к объектам Kaspersky Security для Windows Server проверяет их.                                                                                                                                                                                                                                                                           |
| Эвристический анализатор                                                                  | Применяется уровень безопасности <b>Средний</b> .                                        | Вы можете включать и выключать эвристический анализатор, а также регулировать уровень анализа.                                                                                                                                                                                                                                                                                                            |
| Применять доверенную зону                                                                 | Применяется.                                                                             | Единый список исключений, который можно применять в выбранных задачах.                                                                                                                                                                                                                                                                                                                                    |
| Использовать KSN для защиты                                                               | Применяется.                                                                             | Вы можете увеличить эффективность защиты устройства с помощью облачных служб Kaspersky Security Network (доступных, если принято Положение о KSN).                                                                                                                                                                                                                                                        |
| Расписание запуска задачи                                                                 | При запуске программы.                                                                   | Вы можете настроить запуск задачи по расписанию.                                                                                                                                                                                                                                                                                                                                                          |
| Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность | Не применяется.                                                                          | Вы можете добавлять узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.                                                                                                                                                                                                                                                                                             |
| Запускать проверку важных областей при обнаружении активного заражения                    | Применяется.                                                                             | При обнаружении активного заражения Kaspersky Security для Windows Server создает и запускает временную задачу Проверка важных областей.                                                                                                                                                                                                                                                                  |

## Управление задачей Постоянная защита файлов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

### В этом разделе

|                                                                                |                     |
|--------------------------------------------------------------------------------|---------------------|
| Навигация .....                                                                | <a href="#">302</a> |
| Настройка задачи Постоянная защита файлов .....                                | <a href="#">303</a> |
| Создание и настройка области защиты задачи .....                               | <a href="#">309</a> |
| Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ..... | <a href="#">310</a> |
| Настройка параметров безопасности вручную .....                                | <a href="#">310</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| Переход к параметрам политики для задачи Постоянная защита файлов ..... | <a href="#">302</a> |
| Переход к параметрам задачи Постоянная защита файлов .....              | <a href="#">303</a> |

## Переход к параметрам политики для задачи Постоянная защита файлов

► Чтобы перейти к параметрам задачи *Постоянная защита файлов* в политике *Kaspersky Security Center*, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита сервера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.  
Откроется окно **Постоянная защита файлов**.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

## Переход к параметрам задачи Постоянная защита файлов

► Чтобы перейти к окну параметров задачи **Постоянная защита файлов** для отдельного устройства, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
  - двойным щелчком мыши на имени защищаемого устройства;
  - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. В блоке **Задачи** выберите задачу **Постоянная защита файлов**.
6. Нажмите на кнопку **Свойства**.

Откроется окно **Свойства: Постоянная защита файлов**.

## Настройка задачи Постоянная защита файлов

► Чтобы настроить параметры задачи **Постоянная защита файлов**, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. Настройте следующие параметры задачи:
  - На закладке **Общие**:
    - **Режим защиты объектов** (см. раздел "Выбор режима защиты" на стр. [304](#))
    - **Эвристический анализатор**
    - **Интеграция с другими компонентами** (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. [305](#))
  - На закладке **Управление задачами**:
    - **Запуск задачи по расписанию** (см. раздел "Настройка расписания запуска задач" на стр. [142](#)).
3. Выберите закладку **Область защиты** и выполните следующие действия:
  - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Создание области защиты" на стр. [324](#)).

- В открывшемся окне выберите, что требуется включить в область защиты задачи:
  - **Стандартная область**
  - **Диск, папка или сетевой объект**
  - **Файл**
- Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. [296](#)) или настройте параметры безопасности вручную (см. раздел "Настройка параметров безопасности вручную" на стр. [310](#)).

4. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

|                                                                                         |                     |
|-----------------------------------------------------------------------------------------|---------------------|
| Выбор режима защиты .....                                                               | <a href="#">304</a> |
| Настройка эвристического анализатора и интеграции с другими компонентами программы..... | <a href="#">305</a> |
| Настройка расписания запуска задач .....                                                | <a href="#">307</a> |

## Выбор режима защиты

В задаче **Постоянная защита файлов** вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Security для Windows Server проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► *Чтобы выбрать режим защиты, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
  - **Интеллектуальный режим**

Kaspersky Security для Windows Server выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Security для Windows Server повторно проверяет объект только после его последнего сохранения этим процессом.
  - **При открытии и изменении**

Kaspersky Security для Windows Server проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

Этот вариант выбран по умолчанию.
  - **При открытии**



Kaspersky Security для Windows Server проверяет все объекты при их открытии на чтение, выполнение и изменение.

- **При выполнении**

Kaspersky Security для Windows Server проверяет файл только при открытии на выполнение.

3. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

## Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи **Использование KSN** необходимо принять **Положение о Kaspersky Security Network**.

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".  
Этот уровень выбран по умолчанию.
- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический**

## анализатор.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

- Установите или снимите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать KSN для защиты**.

Этот флажок включает или выключает использование служб KSN.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача не использует службы KSN.

По умолчанию флажок установлен.

Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи **Использование KSN**.

- Установите или снимите флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**.
- Снимите или установите флажок **Запускать проверку важных областей при обнаружении активного заражения**.

Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Security для Windows Server удаляет эту временную задачу.

Если флажок не установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server не создает и не запускает задачу Проверка важных областей.

По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

1. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

## Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

► Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - двойным щелчком мыши по имени задачи;
  - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - а. в списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
    - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
    - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).

- **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
  - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
- b. В поле **Время запуска** укажите время первого запуска задачи.
  - c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [110](#)).

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
  - В блоке **Параметры остановки задачи**:
    - a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
    - b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
  - В блоке **Дополнительные параметры**:
    - a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
    - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
    - c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [129](#).

## Создание и настройка области защиты задачи

► Чтобы создать и настроить область защиты задачи в Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. Выберите закладку **Область защиты**.
3. Все элементы, на которые распространяется область защиты задачи, перечислены в таблице **Область защиты**.
4. Нажмите на кнопку **Добавить**, чтобы добавить в список новый элемент.  
Откроется окно **Добавление объектов в область защиты**.
5. Выберите тип объектов для добавления в область защиты:
  - **Стандартная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
  - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
  - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

6. Чтобы исключить отдельные элементы из области защиты, снимите флажки рядом с именами этих элементов или выполните следующие действия:
  - a. Откройте контекстное меню области защиты по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить исключение**.
  - c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
7. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
8. Чтобы скрыть добавленную ранее область защиты или исключение в списке сетевых файловых ресурсов, в контекстном меню требуемой области защиты выберите пункт **Удалить из списка**.

Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.

9. Нажмите на кнопку **ОК**.

Окно Параметры области защиты закроется. Настроенные параметры будут сохранены.

Задачу **Постоянная защита файлов** можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

## Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранного в дереве файловых ресурсов узла можно задать один из следующих стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** или **Максимальная защита**.

► Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Свойства: Постоянная защита файлов** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. [303](#)).
2. Выберите закладку **Область защиты**.
3. В списке защищаемых устройств выберите элемент, включенный в область защиты, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

Откроется окно **Параметры постоянной защиты файлов**.

5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Свойства: Постоянная защита файлов**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

## Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. [296](#)).

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

► Чтобы вручную настроить параметры безопасности выбранного узла, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).

2. На закладке **Область защиты** выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

Откроется окно **Параметры постоянной защиты файлов**.

3. На закладке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями:
  - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. [311](#))
  - Действия (см. раздел "Настройка действий" на стр. [314](#))
  - Производительность (см. раздел "Настройка производительности" на стр. [316](#))

5. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Новые параметры области защиты будут сохранены.

## В этом разделе

|                                         |                     |
|-----------------------------------------|---------------------|
| Настройка общих параметров задачи ..... | <a href="#">311</a> |
| Настройка действий.....                 | <a href="#">314</a> |
| Настройка производительности .....      | <a href="#">316</a> |

## Настройка общих параметров задачи

- Чтобы настроить общие параметры безопасности задачи **Постоянная защита файлов**, выполните следующие действия.

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите типы объектов, которые вы хотите включить в область защиты:

- **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Проверять загрузочные секторы дисков и MBR**

Включение защиты загрузочных секторов дисков и основных загрузочных записей.

Если флажок установлен, Kaspersky Security для Windows Server проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

По умолчанию флажок установлен.

4. В блоке параметров **Производительность** установите или снимите флажок **Защищать только новые и измененные файлы**.

Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Security для Windows Server новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет и защищает файлы, независимо от того, когда они были изменены.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстрое действие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все / Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:

- **Все / Только новые архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.



- **Все / Только новые SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

Проверка файлов почтовых баз Microsoft Outlook® и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

► Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**

Если выбран этот вариант, Kaspersky Security для Windows Server блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

Выберите действие из раскрывающегося списка:

- **Лечить**
- **Лечить. Удалять, если не удалось вылечить**
- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Выберите действие над возможно зараженными объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными*

*настройками не было предпринято действий для нейтрализации обнаруженного объекта. В событии указана все доступная информация об обнаруженном объекте.*

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**

Если выбран этот вариант, Kaspersky Security для Windows Server блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

Выберите действие из раскрывающегося списка:

- **Помещать на карантин**

- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
  - a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.
 

Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Security для Windows Server не позволит открыть или запустить зараженный объект независимо от вашего выбора.

Если флажок снят, Kaspersky Security для Windows Server выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.
  - b. Нажмите на кнопку **Настройка**.
  - c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
  - d. Нажмите на кнопку **ОК**.
2. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно

зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

3. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

- *Чтобы настроить параметры производительности задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. [302](#)).

2. Выберите закладку **Производительность**.

3. В блоке **Исключения**:

- Снимите или установите флажок **Исключать файлы**.

Исключение файлов из проверки по имени файла или маске имени файла.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server проверяет все объекты.

По умолчанию флажок снят.

- Снимите или установите флажок **Не обнаруживать**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта

ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Не проверять составные объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

Если флажок снят, Kaspersky Security для Windows Server проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Security для Windows Server проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

По умолчанию флажок установлен.

- **Использовать технологию iChecker**

iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Security для Windows Server проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

## Управление задачей Постоянная защита файлов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| Навигация .....                                  | <a href="#">318</a> |
| Настройка задачи Постоянная защита файлов .....  | <a href="#">319</a> |
| Формирование области защиты .....                | <a href="#">324</a> |
| Настройка параметров безопасности вручную .....  | <a href="#">328</a> |
| Статистика задачи Постоянная защита файлов ..... | <a href="#">336</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

## В этом разделе

|                                                                            |                     |
|----------------------------------------------------------------------------|---------------------|
| Переход к параметрам задачи Постоянная защита файлов .....                 | <a href="#">318</a> |
| Переход к параметрам области действия задачи Постоянная защита файлов..... | <a href="#">318</a> |

### Переход к параметрам задачи Постоянная защита файлов

► Чтобы перейти к окну общих параметров задачи, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

### Переход к параметрам области действия задачи Постоянная защита файлов

► Чтобы перейти к окну параметров области защиты для задачи *Постоянная защита файлов*, выполните следующие действия.

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Настройка области защиты**.

Откроется окно **Параметры области защиты**.

## Настройка задачи Постоянная защита файлов

► Чтобы настроить параметры задачи **Постоянная защита файлов**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. [318](#)).
2. На закладке **Общие** настройте следующие параметры задачи:
  - **Режим защиты объектов** (см. раздел "Выбор режима защиты" на стр. [319](#))
  - **Эвристический анализатор**
  - **Интеграция с другими компонентами** (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. [320](#))
3. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)).
4. В окне **Параметры задачи** нажмите на кнопку **ОК**.  
Изменения параметров задачи будут сохранены.
5. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
6. Выполните следующие действия:
  - В дереве или списке файловых ресурсов устройства выберите узлы или элементы, которые вы хотите включить в область защиты задачи.
  - Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. [296](#)) или настройте параметры безопасности вручную (см. раздел "Настройка параметров безопасности" на стр. [548](#)).
7. В окне **Параметры области защиты** нажмите на кнопку **Сохранить**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

### В этом разделе

|                                                                                          |                     |
|------------------------------------------------------------------------------------------|---------------------|
| Выбор режима защиты объектов .....                                                       | <a href="#">319</a> |
| Настройка эвристического анализатора и интеграции с другими компонентами программы ..... | <a href="#">320</a> |
| Настройка расписания запуска задач .....                                                 | <a href="#">323</a> |

## Выбор режима защиты объектов

В задаче **Постоянная защита файлов** вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Security для Windows Server проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► Чтобы выбрать режим защиты, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. [318](#)).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:

- **Интеллектуальный режим**

Kaspersky Security для Windows Server выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Security для Windows Server повторно проверяет объект только после его последнего сохранения этим процессом.

- **При открытии и изменении**

Kaspersky Security для Windows Server проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

Этот вариант выбран по умолчанию.

- **При открытии**

Kaspersky Security для Windows Server проверяет все объекты при их открытии на чтение, выполнение и изменение.

- **При выполнении**

Kaspersky Security для Windows Server проверяет файл только при открытии на выполнение.

3. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

## Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

► Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. [318](#)).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.



Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

- Установите или снимите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

По ссылке **Доверенная зона** перейдите к параметрам доверенной зоны.

- Установите или снимите флажок **Использовать KSN для защиты**.

Этот флажок включает или выключает использование служб KSN.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача не использует службы KSN.

По умолчанию флажок установлен.

Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи **Использование KSN**.

- Установите или снимите флажок **Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность**.

Флажок включает или выключает добавление узлов, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.

Если флажок установлен, Kaspersky Security для Windows Server добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.

Если флажок снят, Kaspersky Security для Windows Server не добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.

По умолчанию флажок снят.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

- Снимите или установите флажок **Запускать проверку важных областей при обнаружении активного заражения**.

Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Security для Windows Server удаляет эту временную задачу.

Если флажок не установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server не создает и не запускает задачу Проверка важных областей.

По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

1. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► Чтобы настроить расписание запуска задачи, выполните следующие действия:

1. Откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
    - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
    - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
    - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
    - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
  - b. В поле **Время запуска** укажите время первого запуска задачи.
  - c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
  - В блоке **Параметры остановки задачи**:
    - a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).

- b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
- В блоке **Дополнительные параметры**:
  - a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
  - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
  - c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **ОК**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

## Формирование области защиты

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Постоянная защита файлов и дальнейшей работе с ней.

### В этом разделе

|                                                       |                     |
|-------------------------------------------------------|---------------------|
| Настройка отображения сетевых файловых ресурсов ..... | <a href="#">324</a> |
| Формирование области защиты .....                     | <a href="#">325</a> |
| Включение сетевых объектов в область защиты .....     | <a href="#">326</a> |
| Формирование виртуальной области защиты.....          | <a href="#">327</a> |

## Настройка отображения сетевых файловых ресурсов

► Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области защиты, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
  - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
  - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

3. Нажмите на кнопку **Сохранить**.

## Формирование области защиты

Процедура формирования области защиты в задаче Постоянная защита файлов зависит от выбранного типа отображения сетевых файловых ресурсов (см. раздел "Об области защиты и параметрах безопасности задачи" на стр. [294](#)). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

Чтобы применить к задаче новые параметры области защиты, нужно перезапустить задачу Постоянная защита файлов.

► Чтобы сформировать область защиты с помощью дерева сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
  - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
  - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
    - Если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с названием нужного типа дисков. Например, чтобы включить все съемные диски устройства, установите флажок **Съемные диски**.
    - Если вы хотите включить в область защиты отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного диска. Например, чтобы выбрать съемный диск F:, разверните узел **Съемные диски** и установите флажок для диска **F:**.
    - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно **Параметры области защиты** закроется. Настроенные параметры будут сохранены.

► Чтобы сформировать область защиты с помощью списка сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
  - a. Откройте контекстное меню области защиты по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить область защиты**.
  - c. В окне **Добавление области защиты** выберите тип объектов, который вы хотите включить в область защиты:

- **Стандартная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
- **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
- **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

3. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
  - a. Откройте контекстное меню области защиты по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить исключение**.
  - c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
4. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
5. Чтобы скрыть добавленную ранее область защиты или исключения в списке сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.

6. Нажмите на кнопку **Сохранить**.

Окно **Параметры области защиты** закрывается. Настроенные параметры будут сохранены.

Задачу Постоянная защита файлов можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Если указана сложная область защиты, например, заданы разные значения параметров безопасности для отдельных узлов в дереве файловых ресурсов устройства, это может привести к замедлению проверки объектов при доступе к ним.

## Включение сетевых объектов в область защиты

Вы можете включать в область защиты сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► Чтобы включить в область защиты сетевой объект, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
  - Выберите пункт **Добавить сетевую папку**, чтобы добавить сетевую папку в область защиты.
  - Выберите пункт **Добавить сетевой файл**, чтобы добавить сетевой файл в область защиты.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention).
5. Нажмите на клавишу **ENTER**.
6. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область защиты.
7. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Формирование виртуальной области защиты

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. [545](#)).

► Чтобы добавить виртуальный диск в область защиты, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню узла **Виртуальные диски**.
4. Выберите пункт **Добавить виртуальный диск**.
5. В списке доступных имен выберите имя создаваемого виртуального диска.
6. Установите флажок рядом с диском, чтобы включить его в область защиты.
7. В окне **Параметры области защиты** нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.



► Чтобы включить в область защиты виртуальную папку или виртуальный файл, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
  - **Добавить виртуальную папку**, чтобы добавить виртуальную папку в область защиты.
  - **Добавить виртуальный файл**, чтобы добавить виртуальный файл в область защиты.
4. В поле ввода задайте имя папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
6. В окне **Параметры области защиты** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты сервера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. [296](#)).

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

При работе с деревом файловых ресурсов защищаемого устройства параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.  
К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. [169](#)).  
В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. [324](#)), создать область защиты (см. раздел "Формирование области защиты" на стр. [325](#)) и создать виртуальную область защиты (см. раздел "Формирование виртуальной области защиты" на стр. [327](#)).
3. В правой части окна выполните одно из следующих действий:
  - На закладке **Уровень безопасности** выберите уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. [329](#)).



- На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
    - **Общие параметры** (см. раздел "**Настройка общих параметров задачи**" на стр. [330](#))
    - **Действия** (см. раздел "**Настройка действий**" на стр. [332](#))
    - **Производительность** (см. раздел "**Настройка производительности**" на стр. [334](#))
  - 4. В окне **Параметры области защиты** нажмите на кнопку **Сохранить**.
- Новые параметры области защиты будут сохранены.

## В этом разделе

|                                                                                |                     |
|--------------------------------------------------------------------------------|---------------------|
| Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ..... | <a href="#">329</a> |
| Настройка общих параметров задачи .....                                        | <a href="#">330</a> |
| Настройка действий.....                                                        | <a href="#">332</a> |
| Настройка производительности .....                                             | <a href="#">334</a> |

## Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** и **Максимальная защита**.

► Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. [318](#)).
2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область защиты.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.

5. Нажмите на кнопку **Сохранить**.

Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

## Настройка общих параметров задачи

► Чтобы настроить общие параметры безопасности задачи *Постоянная защита файлов*, выполните следующие действия.

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи *Постоянная защита файлов*" на стр. [318](#)).

2. Выберите закладку **Общие**.

3. В блоке **Защита объектов** укажите объекты, которые требуется включить в область защиты:

- **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Проверять загрузочные секторы дисков и MBR**

Включение защиты загрузочных секторов дисков и основных загрузочных записей.

Если флажок установлен, Kaspersky Security для Windows Server проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

По умолчанию флажок установлен.

4. В блоке параметров **Производительность** установите или снимите флажок **Защищать только новые и измененные файлы**.

Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky

Security для Windows Server новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет и защищает файлы, независимо от того, когда они были изменены.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстроедействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все / Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:

- **Все / Только новые архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

Проверка файлов почтовых баз Microsoft Outlook® и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

► *Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**

Если выбран этот вариант, Kaspersky Security для Windows Server блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

Выберите действие из раскрывающегося списка:

- **Лечить**
- **Лечить. Удалять, если не удалось вылечить**
- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Выберите действие над возможно зараженными объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**

Если выбран этот вариант, Kaspersky Security для Windows Server блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

Выберите действие из раскрывающегося списка:

- **Помещать на карантин**
- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

- a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Security для Windows Server не позволит открыть или запустить зараженный объект независимо от вашего выбора.

Если флажок снят, Kaspersky Security для Windows Server выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.

- b. Нажмите на кнопку **Настройка**.
  - c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
  - d. Нажмите на кнопку **ОК**.
2. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

3. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

- Чтобы настроить параметры производительности задачи *Постоянная защита файлов*, выполните следующие действия:

1. Откройте окно **Параметры области защиты** (см. раздел "Переход к параметрам области действия задачи Постоянная защита файлов" на стр. [318](#)).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
  - Снимите или установите флажок **Исключать файлы**.

Исключение файлов из проверки по имени файла или маске имени файла.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server проверяет все объекты.

По умолчанию флажок снят.

- Снимите или установите флажок **Не обнаруживать**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

#### 4. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Не проверять составные объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

Если флажок снят, Kaspersky Security для Windows Server проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Security для Windows Server проверяет объекты



файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

По умолчанию флажок установлен.

- **Использовать технологию iChecker**

iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Security для Windows Server проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

## Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Security для Windows Server с момента запуска задачи.

► Чтобы просмотреть статистику задачи Постоянная защита файлов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Постоянная защита файлов**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, обработанных Kaspersky Security для Windows Server с момента запуска задачи (см. таблицу ниже).

Table 57. Статистика задачи Постоянная защита файлов

| Поле                                               | Описание                                                                                                                                                                                                                                                    |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обнаружено</b>                                  | Количество объектов, которые обнаружила программа Kaspersky Security для Windows Server. Например, если программа Kaspersky Security для Windows Server обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.       |
| <b>Зараженных и других обнаруживаемых объектов</b> | Количество объектов, которые программа Kaspersky Security для Windows Server признала зараженными, или количество обнаруженных легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным. |
| <b>Возможно зараженных объектов</b>                | Количество объектов, которые программа Kaspersky Security для Windows Server признала возможно зараженными.                                                                                                                                                 |



| Поле                                                 | Описание                                                                                                                                                                                                                                                       |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Объектов не вылечено</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server не вылечила по следующим причинам: <ul style="list-style-type: none"> <li>• Тип обнаруженного объекта не предполагает лечения.</li> <li>• При лечении возникла ошибка.</li> </ul> |
| <b>Объектов не помещено на карантин</b>              | Количество объектов, которые программе Kaspersky Security для Windows Server не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.                                                                                           |
| <b>Объектов не удалено</b>                           | Количество объектов, которые программе Kaspersky Security для Windows Server не удалось удалить, например, если доступ к объекту был заблокирован другой программой.                                                                                           |
| <b>Объектов не проверено</b>                         | Количество объектов в области защиты, которые программе Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.                                                                        |
| <b>Объектов, не помещенных в резервное хранилище</b> | Количество объектов, копии которых программе Kaspersky Security для Windows Server не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске.                                                                           |
| <b>Ошибок обработки</b>                              | Количество объектов, во время обработки которых возникла ошибка задачи.                                                                                                                                                                                        |
| <b>Вылечено объектов</b>                             | Количество объектов, которые вылечила программа Kaspersky Security для Windows Server.                                                                                                                                                                         |
| <b>Помещено на карантин</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server поместила на карантин.                                                                                                                                                            |
| <b>Помещено в резервное хранилище</b>                | Количество объектов, копии которых программа Kaspersky Security для Windows Server сохранила в резервном хранилище.                                                                                                                                            |
| <b>Удалено объектов</b>                              | Количество объектов, которые удалила программа Kaspersky Security для Windows Server.                                                                                                                                                                          |
| <b>Защищенных паролем объектов</b>                   | Количество объектов (например, архивов), которые программа Kaspersky Security для Windows Server пропустила, так как эти объекты защищены паролем.                                                                                                             |
| <b>Поврежденных объектов</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server пропустила, так как их формат искажен.                                                                                                                                            |
| <b>Обработано объектов</b>                           | Общее количество объектов, которые обработала программа Kaspersky Security для Windows Server.                                                                                                                                                                 |

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в разделе **Управление** панели результатов.

Если значение в поле **Всего событий** в окне журнала выполнения задачи Постоянная защита файлов больше 0, рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

## Управление задачей Постоянная защита файлов с помощью Веб-плагина

С помощью Веб-плагина нельзя изменить стандартный уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. 310) для задачи Постоянная защита файлов.

► Чтобы настроить задачу *Постоянная защита файлов* с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.
6. Настройте параметры, приведены в следующей таблице.

Table 58. Параметры задачи *Постоянная защита файлов*

| Параметр                        | Описание                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Интеллектуальный режим</b>   | Kaspersky Security для Windows Server выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Security для Windows Server повторно проверяет объект только после его последнего сохранения этим процессом. |
| <b>При открытии</b>             | Kaspersky Security для Windows Server проверяет все объекты при их открытии на чтение, выполнение и изменение.                                                                                                                                                                                                                                                 |
| <b>При открытии и изменении</b> | Kaspersky Security для Windows Server проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.<br><br>Этот вариант выбран по умолчанию.                                                                                                                                                                                        |
| <b>При выполнении</b>           | Kaspersky Security для Windows Server проверяет файл только при открытии на выполнение.                                                                                                                                                                                                                                                                        |

| Параметр                                     | Описание                                                                                                                                                                                                                                                                 |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Использовать эвристический анализатор</b> | <p>Флажок включает или выключает использование эвристического анализатора при проверке объектов.</p> <p>Если флажок установлен, эвристический анализатор включен.</p> <p>Если флажок снят, эвристический анализатор выключен.</p> <p>По умолчанию флажок установлен.</p> |

| Параметр                              | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Уровень эвристического анализа</b> | <p>Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.</p> <p>Существуют следующие уровни детализации проверки:</p> <ul style="list-style-type: none"> <li>• <b>Поверхностный.</b> Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.</li> <li>• <b>Средний.</b> Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".<br/>Этот уровень выбран по умолчанию.</li> <li>• <b>Глубокий.</b> Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.</li> </ul> <p>Параметр доступен, если установлен флажок <b>Использовать эвристический анализатор</b>.</p> |

| Параметр                           | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Применять доверенную зону</b>   | <p>Флажок включает или выключает применение доверенной зоны в работе задачи.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.</p> <p>По умолчанию флажок установлен.</p> |
| <b>Использовать KSN для защиты</b> | <p>Этот флажок включает или выключает использование служб KSN.</p> <p>Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.</p> <p>Если флажок снят, задача не использует службы KSN.</p> <p>По умолчанию флажок установлен.</p>                                                                                                         |

| Параметр                                                                                         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Блокировать доступ к общим сетевым ресурсам для узлов, проявляющих вредоносную активность</b> | <p>Флажок включает или выключает добавление узлов, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.</p> <p>По умолчанию флажок снят.</p> <p>Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.</p> <p>Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.</p> |
| <b>Запускать проверку важных областей при обнаружении активного заражения</b>                    | <p>Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Security для Windows Server удаляет эту временную задачу.</p> <p>Если флажок не установлен, то при обнаружении активного заражения Kaspersky Security для Windows Server не создает и не запускает задачу Проверка важных областей.</p> <p>По умолчанию флажок установлен.</p>                                                                                                                                                                                                                                                                                                                                    |
| <b>Область защиты</b>                                                                            | Можно настроить параметры безопасности для области защиты (см. раздел "Настройка параметров безопасности вручную" на стр. <a href="#">310</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

# Проверка скриптов

Этот раздел содержит информацию о задаче Проверка скриптов и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

|                                                                                  |                     |
|----------------------------------------------------------------------------------|---------------------|
| О задаче Проверка скриптов .....                                                 | <a href="#">343</a> |
| Параметры задачи Проверка скриптов по умолчанию.....                             | <a href="#">344</a> |
| Настройка параметров задачи Проверка скриптов с помощью Плагина управления ..... | <a href="#">344</a> |
| Настройка параметров задачи Проверка скриптов с помощью Консоли программы .....  | <a href="#">346</a> |
| Настройка параметров задачи Проверка скриптов с помощью Веб-плагина .....        | <a href="#">347</a> |
| Статистика задачи Проверка скриптов .....                                        | <a href="#">349</a> |

## О задаче Проверка скриптов

В ходе выполнения задачи Проверка скриптов Kaspersky Security для Windows Server контролирует выполнение скриптов, созданных по технологиям Microsoft Windows Script Technologies (Active Scripting), например, скриптов VBScript или JScript®. Программа может также обрабатывать скрипты PowerShell™ и скрипты, работающие в программах Microsoft Office в операционных системах с установленным компонентом Antimalware Scan Interface (далее "AMSI"). Можно разрешить или запретить исполнение опасных или предположительно опасных скриптов. Если программа Kaspersky Security для Windows Server признала скрипт предположительно опасным, она выполняет выбранное вами действие: запрещает или разрешает выполнение скрипта. Если выбрано действие **Запретить**, программа разрешает выполнение скрипта, только если этот скрипт считается безопасным.

Начиная с операционной системы Microsoft Windows Server 2016, Kaspersky Security для Windows Server поддерживает технологию AMSI. Технология AMSI позволяет интегрировать программы и службы с любым установленным на устройстве антивирусным программным обеспечением, чтобы это программное обеспечение могло перехватывать и проверять все исполняемые скрипты.

По умолчанию компонент Проверка скриптов не устанавливается на защищаемое устройство в составе программы. Если установлен компонент Проверка скриптов, программа регистрируется как поставщик AMSI-защиты и проверяет исполняемые скрипты.

На устройствах с операционными системами, не поддерживающими технологию AMSI, использование этого компонента может оказаться несовместимым с некоторыми сторонними программами, установленными на защищаемом устройстве. В этом случае проверка сторонних скриптов может приводить к ошибкам в работе этих скриптов. Рекомендуется либо отказаться от использования сторонних программ, либо остановить задачу Проверка скриптов. Если задача остановлена, возрастают риски, связанные с безопасностью выполнения скриптов.

Если вы хотите использовать компонент Проверка скриптов, вам нужно выбрать его в списке устанавливаемых компонентов вручную во время инсталляции Kaspersky Security для Windows Server. По

умолчанию, если компонент установлен, задача Проверка скриптов запускается автоматически при запуске Kaspersky Security для Windows Server.

Вы можете подробнее ознакомиться с технологией AMSI на сайте Microsoft Windows <https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal>.

Вы можете настраивать параметры задачи Проверка скриптов (см. раздел "Настройка параметров задачи Проверка скриптов с помощью Консоли программы" на стр. [346](#)).

## Параметры задачи Проверка скриптов по умолчанию

По умолчанию системная задача Проверка скриптов имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 59. Параметры задачи Проверка скриптов по умолчанию

| Параметр                               | Значение по умолчанию                             | Описание                                                                                                                            |
|----------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Действия над опасными скриптами</b> | <b>Блокировать</b>                                | Вы можете указывать действия, выполняемые при обнаружении предположительно опасных скриптов: запрещать или разрешать их выполнение. |
| <b>Эвристический анализатор</b>        | Применяется уровень безопасности <b>Средний</b> . | Можно включать и выключать эвристический анализатор. Можно настраивать уровень анализа.                                             |
| <b>Доверенная зона</b>                 | Применяется                                       | Единый список исключений, который можно применять в выбранных задачах.                                                              |

## Настройка параметров задачи Проверка скриптов с помощью Плагина управления

► Чтобы настроить задачу Проверка скриптов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. [124](#)).



- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита сервера** окна **Свойства: <Имя политики>** нажмите на кнопку **Настройка** в подразделе **Проверка скриптов**.
5. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
  - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешить**.  
Kaspersky Security для Windows Server разрешает выполнение предположительно опасных скриптов.
  - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать**.  
Kaspersky Security для Windows Server блокирует выполнение предположительно опасных скриптов.  
Этот вариант выбран по умолчанию.
6. В разделе **Эвристический анализатор** выполните одно из следующих действий:
  - Снимите или установите флажок **Использовать эвристический анализатор**.  
Флажок включает или выключает использование эвристического анализатора при проверке объектов.  
Если флажок установлен, эвристический анализатор включен.  
Если флажок снят, эвристический анализатор выключен.  
По умолчанию флажок установлен.
  - Если требуется, отрегулируйте уровень анализа с помощью ползунка.  
Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.  
Существуют следующие уровни детализации проверки:
    - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
    - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".  
Этот уровень выбран по умолчанию.
    - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность

обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

7. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в задаче.

Если флажок установлен, Kaspersky Security для Windows Server будет учитывать исключения, указанные в списке исключений доверенной зоны с помощью местоположения или с помощью имени или маски имени объекта обнаружения.

Если флажок снят, Kaspersky Security для Windows Server не учитывает исключения при выполнении задачи Проверка скриптов.

По умолчанию флажок установлен.

8. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Настройка параметров задачи Проверка скриптов с помощью Консоли программы

► Чтобы настроить задачу Проверка скриптов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Проверка скриптов**.
3. В панели результатов узла перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи** на закладке **Общие**.

4. В разделе **Действия над опасными скриптами** выполните одно из следующих действий:

- Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешить**.

Kaspersky Security для Windows Server разрешает выполнение предположительно опасных скриптов.

- Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать**.

Kaspersky Security для Windows Server блокирует выполнение предположительно опасных скриптов.

Этот вариант выбран по умолчанию.

5. В разделе **Эвристический анализатор** выполните одно из следующих действий:

- Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

- Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

6. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в задаче.

Если флажок установлен, Kaspersky Security для Windows Server будет учитывать исключения, указанные в списке исключений доверенной зоны с помощью местоположения или с помощью имени или маски имени объекта обнаружения.

Если флажок снят, Kaspersky Security для Windows Server не учитывает исключения при выполнении задачи Проверка скриптов.

По умолчанию флажок установлен.

7. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Настройка параметров задачи Проверка скриптов с помощью Веб-плагина

► Чтобы настроить задачу Проверка скриптов, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.

5. Нажмите на кнопку **Настройка** в подразделе **Проверка скриптов**.
6. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
  - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешить**.

Kaspersky Security для Windows Server разрешает выполнение предположительно опасных скриптов.
  - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать**.

Kaspersky Security для Windows Server блокирует выполнение предположительно опасных скриптов.

Этот вариант выбран по умолчанию.
7. В разделе **Эвристический анализатор** выполните одно из следующих действий:
  - Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.
  - Если требуется, отрегулируйте уровень эвристического анализа.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

    - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
    - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.
    - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
8. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в задаче.

Если флажок установлен, Kaspersky Security для Windows Server будет учитывать исключения, указанные в списке исключений доверенной зоны с помощью

местоположения или с помощью имени или маски имени объекта обнаружения.

Если флажок снят, Kaspersky Security для Windows Server не учитывает исключения при выполнении задачи Проверка скриптов.

По умолчанию флажок установлен.

9. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Статистика задачи Проверка скриптов

В ходе выполнения задачи Проверка скриптов вы можете просматривать информацию о количестве скриптов, обработанных программой Kaspersky Security для Windows Server с момента запуска задачи.

► Чтобы просмотреть статистику задачи Проверка скриптов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Проверка скриптов**.

Текущая статистика задачи отобразится в панели результатов узла, в разделах **Управление** и **Статистика**.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Security для Windows Server обработала за время выполнения задачи (см. таблицу ниже).

Table 60. Статистика задачи Проверка скриптов

| Поле                                                | Описание                                                                    |
|-----------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Заблокировано скриптов</b>                       | Количество скриптов, заблокированных Kaspersky Security для Windows Server. |
| <b>Обнаружено опасных скриптов</b>                  | Количество обнаруженных опасных скриптов.                                   |
| <b>Обнаружено предположительно опасных скриптов</b> | Количество обнаруженных предположительно опасных скриптов.                  |
| <b>Обработано скриптов</b>                          | Общее количество обработанных скриптов.                                     |

# Использование KSN

Этот раздел содержит информацию о задаче Использование KSN и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

|                                                                  |                     |
|------------------------------------------------------------------|---------------------|
| О задаче Использование KSN .....                                 | <a href="#">350</a> |
| Параметры по умолчанию для задачи Использование KSN .....        | <a href="#">352</a> |
| Управление использованием KSN с помощью Плагина управления ..... | <a href="#">353</a> |
| Управление использованием KSN с помощью Консоли программы .....  | <a href="#">357</a> |
| Управление использованием KSN с помощью Веб-плагина .....        | <a href="#">361</a> |
| Настройка передачи дополнительных данных .....                   | <a href="#">364</a> |
| Статистика задачи Использование KSN .....                        | <a href="#">366</a> |

## О задаче Использование KSN

Использование Глобального KSN предполагает передачу данных, описанных в Положении о KSN, на серверы Лаборатории Касперского, и влечет к выходу программы из сертифицированного состояния.

*Kaspersky Security Network* (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security для Windows Server на новые угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Kaspersky Security для Windows Server получает от Kaspersky Security Network только информацию о репутации программ и веб-адресов.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний компонентов программы.

Более подробная информация о передаче, обработке, хранении и уничтожении информации об использовании программы приведена в окне **Обработка данных** задачи Использование KSN и в Политике конфиденциальности на веб-сайте "Лаборатории Касперского".

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Security для Windows Server. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network можно использовать в следующих задачах Kaspersky Security для Windows Server:

- Постоянная защита файлов.
- Проверка по требованию.
- Контроль запуска программ.
- Защита трафика.
- Защита RPC-подключаемых сетевых хранилищ.
- Защита ICAP-подключаемых сетевых хранилищ.

## Kaspersky Private Security Network

Подробнее о том, как настроить Kaspersky Private Security Network (далее также "Локальный KSN"), см. в *Справке Kaspersky Security Center*.

Если вы используете Локальный KSN на устройстве, в окне **Обработка данных** (см. раздел "Настройка обработки данных" на стр. [355](#)) задачи Использование KSN можно ознакомиться с Положением о KSN и включить использование компонента, установив флажок **Я принимаю условия Положения о Kaspersky Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KSN (запросы безопасности, статистические данные), в службы KSN.

После принятия условий Локального KSN флажки, регулирующие использование Глобального KSN, недоступны.

Если вы отключаете Локальный KSN во время выполнения задачи Использование KSN, происходит ошибка *Нарушение лицензии* и выполнение задачи прекращается. Чтобы продолжить защищать устройство, вам нужно принять Положение о KSN в окне **Обработка данных** и перезапустить задачу.

## Отзыв согласия с Положением о KSN

Вы можете отозвать свое согласие и прекратить обмен данными с Kaspersky Security Network в любой момент. Следующие действия считаются полным или частичным отзывом согласия с Положением о KSN:

- Вы сняли флажок **Разрешить отправку данных о проверяемых файлах**: программа перестает отправлять контрольные суммы проверенных файлов в службу KSN для анализа.
- Вы сняли флажок **Разрешить отправку данных о запрашиваемых веб-адресах**: программа перестает отправлять веб-адреса на анализ.

- Вы сняли флажок **Разрешить отправку статистики Kaspersky Security Network**: программа прекращает обрабатывать данные с дополнительной статистикой KSN.
- Вы сняли флажок **Я принимаю условия участия в Kaspersky Security Network**: программа прекращает обрабатывать все связанные с KSN данные, задача Использование KSN останавливается.
- Вы сняли флажок **Я принимаю условия Положения о Kaspersky Managed Protection**: служба КМР будет выключена.
- Вы удалили компонент Использование KSN: обработка всех связанных с KSN данных останавливается.
- Вы удалили Kaspersky Security для Windows Server: обработка всех связанных с KSN данных останавливается.

## Параметры по умолчанию для задачи Использование KSN

Вы можете изменять параметры задачи Использование KSN, заданные по умолчанию (см. таблицу ниже).

Table 61. Параметры по умолчанию для задачи Использование KSN

| Параметр                                                            | Значение по умолчанию                                                                          | Описание                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Действие над объектами, недоверенными в KSN</b>                  | Удалить                                                                                        | Вы можете указывать действия, которые Kaspersky Security для Windows Server будет выполнять над объектами, имеющими репутацию недоверенных в KSN.                                                                                         |
| <b>Отправка данных</b>                                              | Контрольная сумма файла (MD5-хеш) рассчитывается для файлов, размер которых не превышает 2 МБ. | Вы можете указывать максимальный размер файлов, для которых рассчитывается контрольная сумма по алгоритму MD5 для отправки в KSN. Если флажок снят, Kaspersky Security для Windows Server рассчитывает MD5-хеш для файлов любого размера. |
| <b>Расписание запуска задачи</b>                                    | Время первого запуска не задано.                                                               | Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.                                                                                                                                                             |
| <b>Использовать Kaspersky Security Center как прокси-сервер KSN</b> | Выбрано.                                                                                       | По умолчанию все данные отправляются в KSN через Kaspersky Security Center. Этот параметр можно изменять только с помощью Плагина управления.                                                                                             |
| <b>Я принимаю условия Положения о Kaspersky Security Network</b>    | Флажок снят                                                                                    | Если флажок установлен, от вас получено согласие на участие в KSN после установки программы. Вы можете изменить свое решение в любой момент.                                                                                              |



| Параметр                                                        | Значение по умолчанию                                          | Описание                                                                                                                                                            |
|-----------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Разрешить отправку статистики Kaspersky Security Network</b> | Установлен (применяется, только если принято Положение о KSN). | Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок.                                                            |
| <b>Разрешить отправку данных о проверяемых файлах</b>           | Установлен (применяется, только если принято Положение о KSN). | Если Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент. |
| <b>Разрешить отправку данных о запрашиваемых веб-адресах</b>    | Установлен (применяется, только если принято Положение о KSN). | Если приняты условия Положения о KSN, программа отправляет информацию о запрашиваемых веб-адресах в "Лабораторию Касперского".                                      |
| <b>Принять условия Положения о Kaspersky Managed Protection</b> | Флажок снят                                                    | Вы можете включать и выключать службу КМР. Служба доступна, только если во время приобретения программы был подписан дополнительный договор.                        |

## Управление использованием KSN с помощью Плагина управления

В этом разделе описана настройка использования KSN и обработки данных с помощью Плагина управления.

### В этом разделе

|                                                                       |                     |
|-----------------------------------------------------------------------|---------------------|
| Настройка задачи Использование KSN с помощью Плагина управления ..... | <a href="#">353</a> |
| Настройка обработки данных .....                                      | <a href="#">355</a> |

## Настройка задачи Использование KSN с помощью Плагина управления

► Чтобы настроить задачу *Использование KSN*, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита сервера** нажмите на кнопку **Настройка** в подразделе **Использование KSN**.

Откроется окно **Использование KSN**.

5. На закладке **Общие** настройте следующие параметры задачи:

- В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Security для Windows Server при обнаружении объекта, имеющего репутацию недоверенного в KSN:
  - **Удалить**  
Kaspersky Security для Windows Server удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.  
Этот вариант выбран по умолчанию.
  - **Фиксировать информацию в отчете**  
Kaspersky Security для Windows Server фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Security для Windows Server не удаляет недоверенный объект.
- В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
  - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.  
Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.  
Продолжительность расчета контрольной суммы зависит от размера файла.  
Если флажок установлен, Kaspersky Security для Windows Server не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).  
Если флажок снят, Kaspersky Security для Windows Server рассчитывает контрольную сумму для файлов любого размера.  
По умолчанию флажок установлен.
  - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Security для Windows Server будет рассчитывать контрольную сумму.

- В разделе **Прокси-сервер KSN** снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

Флажок позволяет управлять передачей данных от защищаемых устройств в KSN.

Если флажок снят, данные с Сервера администрирования и защищаемых устройств отправляются в KSN напрямую (минуя Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую.

Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center.

По умолчанию флажок установлен.

Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Справке Kaspersky Security Center*.

6. Если требуется, настройте расписание запуска задачи на закладке **Управление задачами**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

Программа будет запускать задачу Использование KSN по расписанию.

7. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных" на стр. [355](#)).
8. Нажмите на кнопку **ОК**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

## Настройка обработки данных

- Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита сервера** нажмите на кнопку **Обработка данных** в подразделе **Использование KSN**.

Откроется окно **Обработка данных KSN**.

5. На закладке **Службы и статистика** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.
6. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

- **Отправлять данные о проверяемых файлах**

Если флажок установлен, Kaspersky Security для Windows Server отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского".  
Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Security для Windows Server не отправляет контрольные суммы файлов в KSN.

Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *Включен "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

По умолчанию флажок установлен.

- **Разрешить отправку данных о проверяемых веб-адресах**

Если флажок установлен, Kaspersky Security для Windows Server отправляет данные о запрашиваемых веб-ресурсах, включая веб-адреса, в "Лабораторию Касперского". Заключение о безопасности запрашиваемых веб-ресурсов основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Security для Windows Server не проверяет репутацию веб-адресов в KSN.

По умолчанию флажок установлен.

Флажок влияет на настройку задачи Защита трафика.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

7. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы программа Kaspersky Security для Windows Server отправляла дополнительную статистику в Лабораторию Касперского.

Если флажок установлен, Kaspersky Security для Windows Server отправляет дополнительную статистику, которая может содержать персональные данные.

Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

Если флажок снят, Kaspersky Security для Windows Server не отправляет дополнительную статистику.

По умолчанию флажок установлен.

8. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Я принимаю условия Положения о Kaspersky Managed Protection**.

Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого устройства специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности.

По умолчанию флажок снят.

При изменении состояния флажка **Я принимаю условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Security для Windows Server.

Для использования службы КМР вам нужно подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом устройстве, а также установить флажки **Я принимаю условия Положения о Kaspersky Security Network**, **Разрешить отправку данных о проверяемых файлах**, **Разрешить отправку данных о проверяемых веб-адресах** и **Разрешить отправку статистики Kaspersky Security Network** на закладке **Службы и статистика KSN**.

9. Нажмите на кнопку **ОК**.

Конфигурация обработки данных будет сохранена.

## Управление использованием KSN с помощью Консоли программы

В этом разделе описана настройка использования KSN и обработки данных с помощью Консоли программы.

### В этом разделе

|                                                                      |                     |
|----------------------------------------------------------------------|---------------------|
| Настройка задачи Использование KSN с помощью Консоли программы ..... | <a href="#">358</a> |
| Настройка обработки данных с помощью Консоли программы .....         | <a href="#">359</a> |

## Настройка задачи Использование KSN с помощью Консоли программы

► Чтобы настроить задачу *Использование KSN*, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
  - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Security для Windows Server при обнаружении объекта, имеющего репутацию недоверенного в KSN:
    - **Удалить**  
Kaspersky Security для Windows Server удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.  
Этот вариант выбран по умолчанию.
    - **Фиксировать информацию в отчете**  
Kaspersky Security для Windows Server фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Security для Windows Server не удаляет недоверенный объект.
  - В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
    - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.  
Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.  
Продолжительность расчета контрольной суммы зависит от размера файла.  
Если флажок установлен, Kaspersky Security для Windows Server не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).  
Если флажок снят, Kaspersky Security для Windows Server рассчитывает контрольную сумму для файлов любого размера.  
По умолчанию флажок установлен.
    - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Security для Windows Server будет рассчитывать контрольную сумму.
5. Если требуется, настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

Программа будет запускать задачу *Использование KSN* по расписанию.

6. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. [359](#)).
7. Нажмите на кнопку **ОК**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

## Настройка обработки данных с помощью Консоли программы

► Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.  
Откроется окно **Обработка данных**.
4. На закладке **Службы и статистика** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.
5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

- **Отправлять данные о проверяемых файлах**

Если флажок установлен, Kaspersky Security для Windows Server отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского".  
Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Security для Windows Server не отправляет контрольные суммы файлов в KSN.

Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *Включен "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

По умолчанию флажок установлен.

- **Разрешить отправку данных о проверяемых веб-адресах**

Если флажок установлен, Kaspersky Security для Windows Server отправляет данные о запрашиваемых веб-ресурсах, включая веб-адреса, в "Лабораторию Касперского". Заключение о безопасности запрашиваемых веб-ресурсов основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Security для Windows Server не проверяет репутацию



веб-адресов в KSN.

По умолчанию флажок установлен.

Флажок влияет на настройку задачи Защита трафика.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

6. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы программа Kaspersky Security для Windows Server отправляла дополнительную статистику в Лабораторию Касперского.

Если флажок установлен, Kaspersky Security для Windows Server отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

Если флажок снят, Kaspersky Security для Windows Server не отправляет дополнительную статистику.

По умолчанию флажок установлен.

7. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Я принимаю условия Положения о Kaspersky Managed Protection**.

Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого устройства специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности.

По умолчанию флажок снят.

При изменении состояния флажка **Я принимаю условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Security для Windows Server.

Для использования службы КМР вам нужно подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом устройстве, а также установить флажки **Я принимаю условия Положения о Kaspersky Security Network**, **Разрешить отправку данных о проверяемых файлах**, **Разрешить отправку данных о проверяемых веб-адресах** и **Разрешить отправку статистики Kaspersky Security Network** на закладке **Службы и статистика KSN**.

8. Нажмите на кнопку **ОК**.

Конфигурация обработки данных будет сохранена.



## Управление использованием KSN с помощью Веб-плаги́на

► Чтобы настроить использование KSN и обработку данных с помощью Веб-плаги́на, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Использование KSN**.
6. Настройте параметры, приведены в следующей таблице.

Table 62. Настройка параметров задачи Использования KSN и обработки данных с помощью Плагина управления

| Параметр                                                                                 | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Удалить</b>                                                                           | Kaspersky Security для Windows Server удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.<br><br>Этот вариант выбран по умолчанию.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Фиксировать информацию в отчете</b>                                                   | Kaspersky Security для Windows Server фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Security для Windows Server не удаляет недоверенный объект.                                                                                                                                                                                                                                                                                                                                         |
| <b>Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает</b> | Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.<br><br>Продолжительность расчета контрольной суммы зависит от размера файла.<br><br>Если флажок установлен, Kaspersky Security для Windows Server не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).<br><br>Если флажок снят, Kaspersky Security для Windows Server рассчитывает контрольную сумму для файлов любого размера.<br><br>По умолчанию флажок установлен. |

| Параметр                                                         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Я принимаю условия Положения о Kaspersky Security Network</b> | Устанавливая этот флажок, вы подтверждаете, что прочитали и принимаете условия Положения о Kaspersky Security Network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Разрешить отправку данных о проверяемых файлах</b>            | <p>Если флажок установлен, Kaspersky Security для Windows Server отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не отправляет контрольные суммы файлов в KSN.</p> <p>Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус <i>Включен "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS</i>.</p> <p>По умолчанию флажок установлен.</p> |

| Параметр                                                        | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Разрешить отправку данных о запрашиваемых веб-адресах</b>    | <p>Если флажок установлен, Kaspersky Security для Windows Server отправляет данные о запрашиваемых веб-ресурсах, включая веб-адреса, в "Лабораторию Касперского". Заключение о безопасности запрашиваемых веб-ресурсов основано на репутации, полученной от KSN.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не проверяет репутацию веб-адресов в KSN.</p> <p>По умолчанию флажок установлен.</p> <p>Флажок влияет на настройку задачи Защита трафика.</p>                                               |
| <b>Разрешить отправку статистики Kaspersky Security Network</b> | <p>Если флажок установлен, Kaspersky Security для Windows Server отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не отправляет дополнительную статистику.</p> <p>По умолчанию флажок установлен.</p> |
| <b>Принять условия Положения о Kaspersky Managed Protection</b> | <p>Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого устройства специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности.</p> <p>По умолчанию флажок снят.</p>                                                                                                                                                                                                             |
| <b>Управление задачами</b>                                      | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Настройка передачи дополнительных данных

В Kaspersky Security для Windows Server можно настроить отправку в "Лабораторию Касперского" следующих данных:

- контрольных сумм проверенных файлов (флажок **Разрешить отправку данных о проверяемых файлах**);
- данных о запрошенных веб-адресах и обработанных сообщениях электронной почты (флажок **Разрешить отправку данных о проверенных веб-адресах**);
- дополнительной статистики, включая персональные данные (флажок **Разрешить отправку статистики Kaspersky Security Network**).

Подробнее о данных, отправляемых в "Лабораторию Касперского", см. в разделе "Локальная обработка данных" этого руководства.

Соответствующие флажки можно установить или снять (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. [359](#)), только если установлен флажок **Я принимаю условия Положения о Kaspersky Security Network**.

По умолчанию Kaspersky Security для Windows Server отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

Table 63. Возможные состояния флажков и соответствующие условия

| Состояние флажка                                                                    | Условия для состояния флажка<br>Разрешить отправку данных о проверяемых файлах                                            | Условия для состояния флажка<br>Разрешить отправку статистики Kaspersky Security Network                                          | Условия для состояния флажка<br>Разрешить отправку данных о проверенных веб-адресах                                                        | Условия для состояния флажка<br>Я принимаю условия Положения о Kaspersky Managed Protection                                                             | Условия для состояния флажка<br>Я принимаю условия Положения о Kaspersky Security Network                                                             |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• отправляются запросы репутации</li> <li>• действия с флажком доступны</li> </ul> | <ul style="list-style-type: none"> <li>• отправляется дополнительная статистика</li> <li>• действия с флажком доступны</li> </ul> | <ul style="list-style-type: none"> <li>• отправляются данные о запрашиваемых веб-адресах</li> <li>• действия с флажком доступны</li> </ul> | <ul style="list-style-type: none"> <li>• принимаются условия Положения о Kaspersky Managed Protection</li> <li>• действия с флажком доступны</li> </ul> | <ul style="list-style-type: none"> <li>• принимаются условия Положения о Kaspersky Security Network</li> <li>• действия с флажком доступны</li> </ul> |

| Состояние флажка                                                                    | Условия для состояния флажка<br>Разрешить отправку данных о проверяемых файлах                                             | Условия для состояния флажка<br>Разрешить отправку статистики Kaspersky Security Network                                           | Условия для состояния флажка<br>Разрешить отправку данных о проверенных веб-адресах                                                         | Условия для состояния флажка<br>Я принимаю условия Положения о Kaspersky Managed Protection                                                              | Условия для состояния флажка<br>Я принимаю условия Положения о Kaspersky Security Network                                                              |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <ul style="list-style-type: none"> <li>отправляются запросы репутации</li> <li>действия с флажком недоступны</li> </ul>    | <ul style="list-style-type: none"> <li>отправляется дополнительная статистика</li> <li>действия с флажком недоступны</li> </ul>    | <ul style="list-style-type: none"> <li>отправляются данные о запрашиваемых веб-адресах</li> <li>действия с флажком недоступны</li> </ul>    | <ul style="list-style-type: none"> <li>принимаются условия Положения о Kaspersky Managed Protection</li> <li>действия с флажком недоступны</li> </ul>    | <ul style="list-style-type: none"> <li>принимаются условия Положения о Kaspersky Security Network</li> <li>действия с флажком недоступны</li> </ul>    |
|  | <ul style="list-style-type: none"> <li>не отправляются запросы репутации</li> <li>действия с флажком доступны</li> </ul>   | <ul style="list-style-type: none"> <li>не отправляется дополнительная статистика</li> <li>действия с флажком доступны</li> </ul>   | <ul style="list-style-type: none"> <li>не отправляются данные о запрашиваемых веб-адресах</li> <li>действия с флажком доступны</li> </ul>   | <ul style="list-style-type: none"> <li>не принимаются условия Положения о Kaspersky Managed Protection</li> <li>действия с флажком доступны</li> </ul>   | <ul style="list-style-type: none"> <li>не принимаются условия Положения о Kaspersky Security Network</li> <li>действия с флажком доступны</li> </ul>   |
|  | <ul style="list-style-type: none"> <li>не отправляются запросы репутации</li> <li>действия с флажком недоступны</li> </ul> | <ul style="list-style-type: none"> <li>не отправляется дополнительная статистика</li> <li>действия с флажком недоступны</li> </ul> | <ul style="list-style-type: none"> <li>не отправляются данные о запрашиваемых веб-адресах</li> <li>действия с флажком недоступны</li> </ul> | <ul style="list-style-type: none"> <li>не принимаются условия Положения о Kaspersky Managed Protection</li> <li>действия с флажком недоступны</li> </ul> | <ul style="list-style-type: none"> <li>не принимаются условия Положения о Kaspersky Security Network</li> <li>действия с флажком недоступны</li> </ul> |

## Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Security для Windows Server обработала с момента ее запуска до текущего момента. Информация обо всех событиях, произошедших во время выполнения задачи, регистрируется в журнале выполнения задачи (см. раздел "О журналах выполнения задач" на стр. [250](#)).

► *Чтобы просмотреть статистику задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Использование KSN**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Security для Windows Server обработала за время выполнения задачи (см. таблицу ниже).

Table 64. Статистика задачи Использование KSN

| Поле                                          | Описание                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Отправлено файловых запросов                  | Количество запросов о репутации файла, отправленных Kaspersky Security для Windows Server в KSN.                                                                                                                                                                                                                                                                           |
| Отправлено запросов о веб-адресе              | Количество запросов о репутации веб-адреса, отправленных Kaspersky Security для Windows Server в KSN.                                                                                                                                                                                                                                                                      |
| Веб-адреса, недоверенные в KSN                | Количество веб-адресов, признанных недоверенными в KSN.                                                                                                                                                                                                                                                                                                                    |
| Недоверенных заключений по файлам             | Количество объектов, признанных недоверенными в KSN.                                                                                                                                                                                                                                                                                                                       |
| Ошибки отправки запросов                      | Количество запросов в KSN, во время обработки которых возникла ошибка задачи.                                                                                                                                                                                                                                                                                              |
| Пакетов статистик сформировано                | Количество пакетов с данными, которые были отправлены на обработку в KSN.                                                                                                                                                                                                                                                                                                  |
| Удалено объектов                              | Количество объектов, которые программа Kaspersky Security для Windows Server удалила в результате выполнения задачи Использование KSN.                                                                                                                                                                                                                                     |
| Помещено в резервное хранилище                | Количество объектов, копии которых программа Kaspersky Security для Windows Server сохранила в резервном хранилище.                                                                                                                                                                                                                                                        |
| Объектов не удалено                           | Количество объектов, которые программа Kaspersky Security для Windows Server попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи.                                                                                                                   |
| Объектов, не помещенных в резервное хранилище | Количество объектов, копии которых программа Kaspersky Security для Windows Server попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи. |
| Ограниченный режим                            | Статус отправки запросов файловой репутации в ограниченном режиме. В ограниченном режиме Kaspersky Security для Windows Server отправляет только часть запросов о репутации файлов, в соответствии с рекомендациями специалистов "Лаборатории Касперского".                                                                                                                |

# Защита трафика

Этот раздел содержит информацию о задаче Защита трафика и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

|                                                               |                     |
|---------------------------------------------------------------|---------------------|
| О задаче Защита трафика .....                                 | <a href="#">368</a> |
| О правилах защиты трафика .....                               | <a href="#">369</a> |
| Защита от почтовых угроз.....                                 | <a href="#">370</a> |
| Список категорий .....                                        | <a href="#">371</a> |
| Параметры стандартных уровней защиты .....                    | <a href="#">375</a> |
| Параметры задачи Защита трафика по умолчанию.....             | <a href="#">377</a> |
| Управление защитой трафика с помощью Плагина управления ..... | <a href="#">377</a> |
| Управление защитой трафика с помощью Консоли программы .....  | <a href="#">393</a> |
| Управление защитой трафика с помощью Веб-плагина .....        | <a href="#">408</a> |

## О задаче Защита трафика

Компонент Защита трафика обрабатывает сетевой трафик, включая трафик, поступающий от почтовых служб, перехватывает и проверяет объекты, передаваемые через веб-трафик, на наличие известных компьютерных и других угроз на защищаемом устройстве. Служба ICAP проверяет входящий трафик на наличие угроз и блокирует или разрешает трафик в зависимости от результатов и настроенных параметров проверки.

Kaspersky Security для Windows Server также обнаруживает и перехватывает трафик, запрошенный с помощью процессов подсистемы Windows для Linux. Для данных целей задача Защита трафика применяет действия, указанные в текущих параметрах.

Компонент Защита трафика установлен по умолчанию.

Компонент обеспечивает следующие типы защиты:

- Защита от почтовых угроз:
  - Антифишинг.
  - Защита от вредоносных программ, передающихся через почтовый трафик.
- Защита от веб-угроз:
  - Антифишинг.
  - Проверка вредоносных веб-адресов.
  - Защита от вредоносных программ, передающихся через веб-трафик.
  - Веб-контроль:
    - Контроль веб-адресов.



- Контроль сертификатов.
- Контроль по веб-категориям.

Настоятельно рекомендуется использовать службы KSN при запуске задачи Защита трафика для улучшения обнаружения угроз. Облачные базы KSN содержат более актуальные данные о веб-угрозах, чем локальные антивирусные базы. Анализ некоторых категорий веб-контроля полностью основан на заключениях, полученных от служб KSN.

## Режимы задачи Защита трафика

Защита трафика может работать в следующих режимах:

- **Драйверный перехват.** Программа перехватывает трафик с помощью сетевого драйвера. Сетевой драйвер используется для перехвата и анализа входящего трафика, поступающего через указанные порты.
- **Перенаправление трафика.** Программа обрабатывает запросы, поступающие от веб-браузера пользователя, как прокси-сервер и перенаправляет полученный трафик на внутренний ICAP-сервер. Этот режим подразумевает дополнительную настройку веб-браузера: вам нужно указать адрес и порт для подключения прокси-сервера.
- **Внешний прокси-сервер.** Программа обрабатывает трафик с внешнего прокси-сервера. Трафик передается с внешнего прокси-сервера в Kaspersky Security для Windows Server. Программа анализирует трафик и рекомендует действие для внешнего прокси-сервера. Программа Kaspersky Security для Windows Server совместима только с прокси-серверами, которые передают трафик по протоколу ICAP.

## О правилах защиты трафика

Kaspersky Security для Windows Server позволяет добавлять и настраивать разрешающие и запрещающие правила для сертификатов и веб-адресов и использовать стандартные правила для категорий, чтобы блокировать контент в зависимости от его типа. Правила для сертификатов можно использовать при режиме выполнения задачи **Драйверный перехват** или **Перенаправление трафика**.

### Веб-контроль

Этот тип контроля реализуется путем применения разрешающих и запрещающих правил для веб-адресов и сертификатов. У разрешающих правил более высокий приоритет, чем у заключений KSN или сигнатурного анализа.

Веб-адрес или сертификат можно разрешить или заблокировать на основе заключения с приоритетом от высокого до низкого:

1. разрешающие и запрещающие правила;
2. антифишинговые и антивирусные базы;
3. KSN;
4. категории.

## Контроль по веб-категориям.

Kaspersky Security для Windows Server позволяет блокировать веб-адреса на основе категорий. Вы можете выбрать уровень эвристического анализа, используемого для категоризации. Контроль по веб-категориям использует для анализа стандартный список категорий. Вы не можете изменять список, но можете выбрать категории веб-ресурсов, которые будут разрешены или заблокированы, или выключить контроль по веб-категориям. Категория Прочие включает все веб-ресурсы, которые не попадают в другие категории из списка. Если этот флажок установлен, Kaspersky Security для Windows Server разрешает все веб-ресурсы, для которых не определена категория. Если флажок снят, все веб-ресурсы блокируются.

У категоризации самый низкий приоритет.

По умолчанию Kaspersky Security для Windows Server применяет только одно правило – запрещающее правило для TOR-сертификатов. Вы можете отключить правило в параметрах правила, чтобы разрешить соединения TOR. Если правило применяется, все входящие и исходящие соединения TOR блокируются.

При защите трафика также учитываются заключения по маске `not-a-virus`, представляющие ресурсы или объекты, которые сами не являются вирусами, но могут быть использованы для нанесения вреда защищаемому устройству. По умолчанию Kaspersky Security для Windows Server не применяет маску `not-a-virus` для категорий (см. раздел "Настройка веб-контроля на основе категорий" на стр. [391](#)).

## Защита от почтовых угроз

Задача Защита трафика проверяет электронную почту для Microsoft Outlook версий 2010, 2013 и 2016 (32-разрядных и 64-разрядных). Защита от почтовых угроз предоставляется через расширение для Microsoft Outlook, которое устанавливается отдельно от компонентов Kaspersky Security для Windows Server.

Защита от почтовых угроз включает:

- проверку входящей электронной почты;
- антивирусную проверку электронной почты;
- антивирусную проверку вложений (включая упакованные объекты);
- антифишинговую проверку электронной почты;
- антифишинговую проверку вложений (включая упакованные объекты).

При обнаружении угрозы Kaspersky Security для Windows Server выполняет следующие действия:

- Полностью удаляет зараженные вложения.
- Изменяет тело зараженного письма. Исходный текст зараженного письма присоединяется к письму как HTML-страница вместе с информацией об угрозе. При обнаружении фишинговой ссылки, исходный текст зараженного письма присоединяется к письму в формате TXT вместе с информацией об угрозе.
- Регистрирует событие *Обнаружена почтовая угроза*.

Kaspersky Security для Windows Server проверяет сообщения электронной почты при открытии, а не при получении сообщения на защищаемом устройстве. Проверка выполняется только один раз, при первом

открытии сообщения. Проверенные сообщения и вложения хранятся в кеше до перезапуска Microsoft Outlook. После перезагрузки сообщения проверяются повторно при открытии.

► *Расширение загружается почтовым клиентом Microsoft Outlook при запуске. Если вы устанавливаете расширение для Microsoft Outlook, когда запущен Microsoft Outlook, выполните следующие действия:*

1. Откройте **Файл > Параметры > Надстройки**.
2. Убедитесь, что расширение для Microsoft Outlook добавлено в один из списков: **Активный** или **Неактивный**.
3. Перезапустите Microsoft Outlook.
4. Проверьте статус расширения для Microsoft Outlook. Статус должен измениться на **Активный**.

## Список категорий

Веб-ресурсы анализируются и распределяются по категориям согласно тегам. Тег может быть присвоен нескольким категориям (см. таблицу ниже).

Table 65. Теги категорий веб-ресурсов

| Тег         | Описание                                                                                                                                                                                | Список категорий                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18+ (adult) | В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы для взрослых (18+), например описания насилия, порнографию или нецензурную брань.                         | Аборт, Знакомства для взрослых, Анорексия, Недовольство, Дискриминация, Эротика, Незаконные препараты, Незаконное скачивание, ЛГБТ, Нижнее белье, Сайты знакомств, Нудизм, Политическое решение, Порно, Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Половое воспитание, Секс-шопы, Социальные сети, Суицид, Нецензурная брань, Жестокость, Оружие. |
| children    | В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы для детей. Например: образовательные сайты, развлекательные сайты для детей, форумы и блоги о воспитании. | Дети, Запрещено Федеральным законом 436 (РФ), Школы и университеты.                                                                                                                                                                                                                                                                                                                                        |

| Тег                 | Описание                                                                                                                                                                                                                                                                                         | Список категорий                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| drug                | В эти категории могут попадать веб-ресурсы, потенциально содержащие информацию о наркотических и других веществах, распространяемых легально или нелегально. Например, данные о распространении запрещенных препаратов, алкоголе или веб-страницы зарегистрированных фармакологических компаний. | Аборт, Алкоголь, Анорексия, Наркотики, Красота и здоровье, Незаконные препараты, Медицина, Фармакология, Табак.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| education           | В эти категории могут попадать веб-ресурсы, потенциально содержащие учебные материалы или посвященные обучению. Например: онлайн-энциклопедии, базы знаний, вики, веб-страницы учебных заведений или страницы о половом воспитании.                                                              | Книги, Образование, Дети, Информационные технологии, Онлайн-энциклопедии, Школы и университеты, Поисковые системы, Половое воспитание.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| hobby&entertainment | В эти категории могут попадать веб-ресурсы, потенциально относящиеся к развлечениям, хобби и свободному времяпрепровождению. Например: онлайн-игры разных типов, включая азартные, социальные сети, страницы о книгах или охоте, блоги о здоровье и красоте или новостные ленты.                 | Знакомства для взрослых, Хобби и развлечения, Онлайн общение, Астрология и эзотерика, Аудио, видео и дистрибутивы, Ставки, Блоги, Казино, Карточные игры, Казуальные игры, Чаты и форумы, Компьютерные игры, Культура, Эротика, Мода, Файлообменники, Охота и рыбалка, Дети, Азартные игры, Красота и здоровье, Хобби и развлечения, Дом и семья, Юмор, ЛГБТ, Нижнее белье, Лотереи, Потокное вещание, Медицина, Музыка, Новости, Сайты знакомств, Нудизм, Онлайн-магазины, Онлайн-шоппинг (собственные системы оплаты), Животные, Порно, Рестораны, кафе и еда, Секс-шопы, Социальные сети, Спорт, Торренты, Путешествия, Радио и телевидение, Военные игры. |
| gaming              | В эти категории могут попадать веб-ресурсы, потенциально имеющие отношение к разным типам игр. Например: азартные игры и ставки, лотереи, сетевые или казуальные игры, а также веб-сайты и форумы на игровую тематику.                                                                           | Казуальные игры, Компьютерные игры, Спорт, Военные игры.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Ter              | Описание                                                                                                                                                                                                                    | Список категорий                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hazard           | В эту категорию входят веб-страницы, которые содержат:<br>Азартные игры в формате «плати и играй».<br>Ставки.<br>Лотереи с необходимостью приобретения билетов.                                                             | Ставки, Казино, карточные игры, Азартные игры, Лотереи.                                                                                                                                                                                  |
| health&medicine  | Веб-страницы о здоровом образе жизни. Могут содержать страницы о фитнесе, здоровом питании, альтернативных практиках и методах лечения; страницы о медицине, фармацевтике, фармацевтических компаниях, аптеках, лекарствах. | Аборт, Анорексия, Наркотики, Незаконные препараты, Красота и здоровье, Медицина, Фармакология, Спорт.                                                                                                                                    |
| illegal          | В эти категории могут попадать потенциально нелегальные веб-ресурсы. Например: нелегальное распространение медиа-файлов или дистрибутивов или страницы, запрещенные официальным законодательством разных стран.             | Алкоголь, Аудио, видео и дистрибутивы, Наркотики, Файлообменники, Незаконные препараты, Незаконное скачивание, Азартные игры, Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Табак. |
| IT               | Веб-ресурсы, которые позволяют пользователям (имеющим и не имеющим аккаунт) обмениваться сообщениями (в том числе, почтовые сервисы, социальные сети, блоги и т.д.)                                                         | Анонимизация, Доменные и хостинговые сервисы, Нелегальные программы, Информационные технологии, Поисковые системы, Почтовые веб-сервисы.                                                                                                 |
| forbidden by law | В эти категории могут попадать веб-ресурсы, потенциально находящиеся под контролем федерального законодательства или имеющие отношение к государственной или политической тематике.                                         | Закон и политика, Упомянуто в Федеральном списке экстремистских материалов (РФ), Запрещено Федеральным законом 436 (РФ), Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ).             |
| legal            | В эти категории могут попадать потенциально легальные веб-ресурсы.                                                                                                                                                          | Алкоголь, Аудио, видео и дистрибутивы, Наркотики, Файлообменники, Легальные рекламные ресурсы, Лотереи, Армия, Фармакология, Религия, Половое воспитание, Реклама, Табак, Военные игры.                                                  |

| Тег                  | Описание                                                                                                                                                                                                                             | Список категорий                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| media sharing        | В эти категории могут попадать веб-ресурсы, потенциально позволяющие совершать файловый обмен.<br>Например: торренты, файлообменники, музыкальные и видео хостинги, как легальные, так и нелегальные.                                | Аудио, видео и дистрибутивы, Книги, Файлообменники, Дети, Онлайн-сервисы, Потоковое вещание, Музыка, Поисковые системы, Торренты, Радио и телевидение.                  |
| money&payment        | В эти категории могут попадать веб-ресурсы, потенциально связанные с финансами и финансовыми операциями.<br>Например: официальные сайты банков, онлайн-банки, онлайн-магазины, а также страницы для совершения денежных переводов.   | Банки, Книги, Казуальные игры, Электронная торговля, Онлайн-шоппинг (собственные системы оплаты), Онлайн-оплата, Платежные системы, Рестораны, кафе и еда, Путешествия. |
| online collaboration | В эти категории могут попадать веб-ресурсы, потенциально связанные с общением в интернете.<br>Например: тематические блоги и форумы, приватные чаты, социальные сети или знакомства для взрослых.                                    | Знакомства для взрослых, Блоги, Чаты и форумы, Дети, Красота и здоровье, Поиск работы, Медицина, Сайты знакомств, Социальные сети, Путешествия.                         |
| psychotropic&drug    | Эти категории могут включать веб-ресурсы, связанные с любыми типами наркотических веществ, психотропных препаратов или табаком.                                                                                                      | Наркотики, Незаконные препараты, Красота и здоровье, Медицина, Фармакология, Табак.                                                                                     |
| sex&adult            | В эти категории могут попадать веб-ресурсы, потенциально содержащие материалы сексуального и эротического характера.<br>Например: порнографические хостинги, страницы о половом воспитании или сайты, посвященные секс-меньшинствам. | Знакомства для взрослых, Эротика, ЛГБТ, Нижнее белье, Нудизм, Порно, Половое воспитание, Секс-шопы.                                                                     |
| society&law          | Эта категория включает множество аспектов жизни общества и человека, включая религию, правительственные организации, законодательство; дом и семью; новости; армию и оружие.                                                         | Культура и общество, Закон и политика, Армия, Религия, Оружие.                                                                                                          |

| Тег          | Описание                                                                                                                                                            | Список категорий                                                                                                                                                                                                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| shopping     | В эти категории могут попадать веб-ресурсы, потенциально относящиеся к онлайн-шоппигу.                                                                              | Книги, Нижнее белье, Онлайн-магазины, Онлайн-шоппиг (собственные системы оплаты), Онлайн-оплата, Рестораны, кафе и еда, Секс-шопы, Путешествия.                                                                                                                                                                                              |
| violence     | В эти категории могут попадать веб-ресурсы, потенциально содержащие прямое выражение агрессии, описания жестокого обращения, пропаганду экстремизма или суицида.    | Недовольство, Дискриминация, Экстремизм и расизм, Охота и рыбалка, Ненависть и дискриминация, Упомянуто в Федеральном списке экстремистских материалов (РФ), Армия, Политическое решение (JP), Запрещено мировым законодательством, Запрещено законодательством РФ, Запрещено Роскомнадзором (РФ), Суицид, Жестокость, Военные игры, Оружие. |
| web services | В эти категории могут попадать веб-ресурсы, потенциально предоставляющие различные веб-сервисы. Например: анонимизация, веб-хостинги или сервисы электронной почты. | Анонимизация, Доменные и хостинговые сервисы, Онлайн-сервисы, Поисковые системы, Реклама, Почтовые веб-сервисы.                                                                                                                                                                                                                              |

## Параметры стандартных уровней защиты

Для выбранного в дереве сетевых файловых ресурсов узла можно задать один из трех стандартных уровней защиты: Максимальное быстродействие, Рекомендуемый и Максимальная защита. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

### Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Security для Windows Server на защищаемых устройствах и рабочих станциях, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

### Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

### Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности устройств в сети организации.

Table 66. Стандартные уровни защиты и соответствующие им параметры безопасности

| Параметры                                                  | Уровень защиты                                                        |                                                                                                                                          |                                                                                                                                          |
|------------------------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | Максимальное быстродействие                                           | Рекомендуемый                                                                                                                            | Максимальная защита                                                                                                                      |
| Проверка объектов                                          | Согласно списку расширений в базе данных                              | Все объекты                                                                                                                              | Все объекты                                                                                                                              |
| Действие над зараженными и другими обнаруженными объектами | Блокировать                                                           | Блокировать                                                                                                                              | Блокировать                                                                                                                              |
| Не обнаруживать                                            | Нет                                                                   | Нет                                                                                                                                      | Нет                                                                                                                                      |
| Останавливать проверку, если она длится более (сек)        | 60 сек.                                                               | 60 сек.                                                                                                                                  | 60 сек.                                                                                                                                  |
| Не проверять объекты размером более (МБ)                   | 20 МБ                                                                 | 20 МБ                                                                                                                                    | Нет                                                                                                                                      |
| Защита составных объектов                                  | <ul style="list-style-type: none"> <li>Упакованные объекты</li> </ul> | <ul style="list-style-type: none"> <li>Архивы</li> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> | <ul style="list-style-type: none"> <li>Архивы</li> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> |



## Параметры задачи Защита трафика по умолчанию

Вы можете изменять параметры задачи Защита трафика, заданные по умолчанию (см. таблицу ниже).

Table 67. Параметры задачи Защита трафика по умолчанию

| Параметр                                                                 | Значение по умолчанию            | Описание                                                                                                                                                                                                    |
|--------------------------------------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Режим работы задачи</b>                                               | Драйверный перехват              | Программа перехватывает трафик с помощью сетевого драйвера. Сетевой драйвер используется для перехвата и анализа входящего трафика, поступающего через указанные порты.                                     |
| <b>Номер сетевого порта</b>                                              | 1345                             | Номер порта ICAP-службы по умолчанию.                                                                                                                                                                       |
| <b>Идентификатор службы</b>                                              | webscan                          | Идентификатор ICAP-службы для адреса установленного антивирусного сервера.                                                                                                                                  |
| <b>Использовать базу вредоносных веб-адресов для проверки веб-ссылок</b> | Применяется.                     | Включает или выключает сигнатурный анализ для каждого веб-адреса.                                                                                                                                           |
| <b>Использовать антифишинговую базу для проверки веб-страниц</b>         | Применяется.                     | Включает или отключает антифишинговую проверку веб-адресов на основе эвристического анализа.                                                                                                                |
| <b>Использовать KSN для защиты</b>                                       | Применяется.                     | Вы можете использовать данные KSN о репутации программ для защиты при выполнении задачи.                                                                                                                    |
| <b>Использование доверенной зоны</b>                                     | Применяется.                     | При необходимости вы можете применить доверенную зону.                                                                                                                                                      |
| <b>Уровень защиты</b>                                                    | Рекомендуемый                    | Для узлов, выбранных в дереве файловых ресурсов защищаемого устройства, можно выполнить следующие действия:<br>применить другой стандартный уровень безопасности;<br>вручную изменить уровень безопасности; |
| <b>Расписание запуска задачи</b>                                         | Время первого запуска не задано. | Задача Защита трафика не запускается автоматически. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.                                                                           |

## Управление защитой трафика с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

## В этом разделе

|                                                      |                     |
|------------------------------------------------------|---------------------|
| Навигация .....                                      | <a href="#">378</a> |
| Настройка задачи Защита трафика .....                | <a href="#">379</a> |
| Настройка антивирусной защиты .....                  | <a href="#">384</a> |
| Настройка защиты от почтовых угроз .....             | <a href="#">387</a> |
| Настройка обработки веб-адресов и веб-контента ..... | <a href="#">388</a> |
| Настройка веб-контроля .....                         | <a href="#">389</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

## В этом разделе

|                                                               |                     |
|---------------------------------------------------------------|---------------------|
| Переход к параметрам политики для задачи Защита трафика ..... | <a href="#">378</a> |
| Переход к списку правил защиты трафика .....                  | <a href="#">379</a> |

## Переход к параметрам политики для задачи Защита трафика

- *Чтобы перейти к параметрам задачи Защита трафика в политике Kaspersky Security Center, выполните следующие действия:*
  1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой вы хотите настроить задачу.
  3. Выберите закладку **Политики**.
  4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.  
В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита сервера**.
  5. Нажмите на кнопку **Настройка** в подразделе **Защита трафика**.  
Откроется окно **Защита трафика**.
  6. Настройте политику в соответствии с вашими требованиями.

## Переход к списку правил защиты трафика

- Чтобы перейти к списку правил Веб-контроля в Kaspersky Security Center, выполните следующие действия:
1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой вы хотите настроить задачу.
  3. Выберите закладку **Политики**.
  4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
  5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита сервера**.
  6. Нажмите на кнопку **Список правил** в подразделе **Защита трафика**.  
Откроется окно **Правила веб-контроля**.
- Настройте список правил в соответствии с вашими требованиями.

## Настройка задачи Защита трафика

- Чтобы настроить задачу **Защита трафика**, выполните следующие действия:
1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
  2. На закладке **Режим работы** выберите и настройте режим работы задачи (см. раздел "Настройка режима работы задачи" на стр. [380](#)).
  3. На закладке **Обработка веб-адресов и веб-контента** настройте антифишинговую и антивирусную проверку веб-адресов (см. раздел "Настройка обработки веб-адресов и веб-контента" на стр. [388](#)).
  4. На закладке **Антивирусная защита** настройте эвристический анализ и уровень безопасности (см. раздел "Настройка антивирусной защиты" на стр. [384](#)).
  5. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. [141](#)).
  6. Нажмите на кнопку **ОК**.
- Параметры задачи будут сохранены.

### В этом разделе

|                                                |                     |
|------------------------------------------------|---------------------|
| Настройка режима работы задачи .....           | <a href="#">380</a> |
| Настройка режима Драйверный перехват .....     | <a href="#">380</a> |
| Настройка режима Перенаправление трафика ..... | <a href="#">382</a> |

## Настройка режима работы задачи

► Чтобы настроить режим работы задачи, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
2. На закладке **Общие** выберите один из доступных режимов в раскрывающемся списке **Режим работы задачи**:
  - **Драйверный перехват** (см. раздел "Настройка режима Драйверный перехват" на стр. [380](#))
  - **Перенаправление трафика** (см. раздел "Настройка режима Перенаправление трафика" на стр. [382](#))
  - **Внешний прокси-сервер**
3. Укажите параметры соединения службы ICAP (требуется для всех трех режимов):
  - **Номер сетевого порта**  
Номер порта ICAP службы Kaspersky Security для Windows Server.
  - **Идентификатор службы**  
Идентификатор, который является частью параметра RESPMOD URI протокола ICAP (см. документ RFC 3507). RESPMOD URI обозначает адрес антивирусного ICAP-сервера, установленный для сетевого хранилища.  
  
Например, если IP-адрес защищаемого устройства – 192.168.10.10, номер порта – 1345, а идентификатор ICAP-службы – webscan, эти параметры соответствуют следующему адресу RESPMOD URI – icap://192.168.10.10/webscan:1345.

Перезапустите задачу, чтобы применить параметры подключения ICAP-службы.

4. Настройте выбранный режим работы задачи.

Для режима **Внешний прокси-сервер** дополнительная настройка не требуется. Настройка выполняется на стороне внешнего прокси-сервера.

5. Нажмите на кнопку **ОК**.

Параметры будут сохранены.

## Настройка режима Драйверный перехват

► Чтобы настроить режим Драйверный перехват, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
2. На закладке **Общие** выберите режим **Драйверный перехват**.
3. В блоке **Параметры режима работы** настройте следующие параметры:
  - **Проверять безопасные соединения по протоколу HTTPS**

Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:

- TLS 1.0;
- TLS 1.1;
- TLS 1.2.

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче Защита трафика только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

- **Не доверять веб-серверам с недействительными сертификатами**

Этот флажок доступен, только если установлен флажок **Проверять безопасные соединения по протоколу HTTPS**.

Если этот флажок установлен, веб-страница с недействительным сертификатом блокируется (например, если закончился срок действия сертификата, возникла ошибка проверки подписи, сертификат отозван и т. д.).

- **Порт безопасности**

Укажите номер порта, используемого для перенаправления трафика из браузера или сетевого драйвера на внутренний порт Kaspersky Security для Windows Server для обнаружения веб-угроз. Не рекомендуется изменять порт, указанный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если используется режим **Перенаправление трафика**, используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.

4. Чтобы добавить порты в область перехвата или исключить из нее, нажмите на кнопку **Настроить область перехвата**.

Откроется окно **Область перехвата**.

5. На закладке **Перехватывать по портам** выберите один из следующих вариантов:

- **Перехватывать все**
- **Перехватывать по указанным портам**

- a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.

- b. Нажмите на кнопку **Добавить**.

Порт будет включен в область перехвата.

По умолчанию Kaspersky Security для Windows Server перехватывает трафик, передаваемый через следующие порты: 80, 8080, 3128, 443.

6. Чтобы указать порты, которые требуется исключить из области перехвата, на закладке **Исключить порты** выполните следующие действия:

- a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.
- b. Нажмите на кнопку **Добавить**.

Порт будет исключен из области перехвата.

По умолчанию Kaspersky Security для Windows Server исключает порты, которые используются другими программами и могут вызывать проблемы при попытке просмотра содержимого, передаваемого по зашифрованному соединению: 3389, 1723, 13291.

7. Чтобы исключить IP-адреса из области перехвата, на закладке **Исключить IP-адреса** выполните следующие действия:

- a. Введите IP-адрес в формате IPv4 (в краткой форме или указав адрес с помощью маски подсети).
- b. Нажмите на кнопку **Добавить**.
- c. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

8. Чтобы исключить процесс или исполняемый файл, который требует обмена трафиком, на закладке **Исключить процессы** выполните следующие действия:

- a. Установите флажок **Применять исключения для процессов**.

- b. Чтобы исключить файл, выполните следующие действия:

1. Нажмите на кнопку **Исполняемые файлы**.

Отобразится стандартное окно **Открыть**.

2. Выберите исполняемый файл, который хотите исключить, и нажмите **Открыть**.

9. В окне **Область перехвата** нажмите на кнопку **ОК**.

10. В окне **Защита трафика** нажмите на кнопку **ОК**.

Параметры режима работы задачи будут сохранены.

## Настройка режима Перенаправление трафика

► Чтобы настроить режим *Перенаправление трафика*, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
2. На закладке **Общие** выберите режим **Перенаправление трафика**.
3. В блоке **Параметры режима работы** настройте следующие параметры:

- **Проверять безопасные соединения по протоколу HTTPS**

Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик

и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:

- TLS 1.0;
- TLS 1.1;
- TLS 1.2.

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче Защита трафика только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

- **Перенаправлять трафик на прокси-сервер после проверки**

Если флажок установлен, Kaspersky Security для Windows Server перенаправляет уже проверенный трафик на внешний прокси-сервер, например, на корпоративный прокси-сервер, используемый в сети организации.

Если флажок снят, трафик направляется на внутренний прокси-сервер.

- **Адрес прокси-сервера**

Адрес внутреннего терминального прокси-сервера для перенаправления трафика. Введите адрес в формате IPv4.

- **Порт**

Номер порта для внутреннего прокси-сервера.

- **Порт безопасности**

Укажите номер порта, используемого для перенаправления трафика из браузера или сетевого драйвера на внутренний порт Kaspersky Security для Windows Server для обнаружения веб-угроз. Не рекомендуется изменять порт, указанный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если используется режим **Перенаправление трафика**, используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.

Для режима **Перенаправление трафика** в операционной системе должно быть настроено перенаправление зашифрованного трафика через порт, указанный в Kaspersky Security для Windows Server.

4. Нажмите на кнопку **ОК**.

Параметры режима работы задачи будут сохранены.

## Настройка антивирусной защиты

Следующие параметры защиты влияют на весь входящий трафик. Однако выбранные действия над зараженными и прочими обнаруженными объектами выполняются только для почтовых вложений. Задача Защита трафика передает в Kaspersky Sandbox только файлы документов.

► Чтобы настроить эвристический анализ для обнаружения вирусов и других угроз компьютерной безопасности, передаваемых через веб-трафик, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
2. На закладке **Антивирусная защита** выполните следующие действия:

- Установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

- Установите флажок **Использовать эвристический анализатор**.
  - Выберите нужный уровень эвристического анализа для антивирусной проверки.
  - Выберите уровень безопасности (см. раздел "Параметры стандартных уровней безопасности" на стр. [375](#)) из раскрывающегося списка:
    - **Рекомендуемый**
    - **Максимальная защита**
    - **Максимальное быстродействие**
    - **Пользовательский**
3. Откройте закладку **Общие** по кнопке **Настройка** и в разделе **Защита объектов** укажите объекты, которые вы хотите включить в область проверки:
    - **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.



- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- а. Нажмите на кнопку **Изменить**, чтобы изменить список расширений.
- б. В открывшемся окне укажите расширение.
- в. Нажмите на кнопку **Добавить**.

Нажмите на кнопку **По умолчанию**, чтобы добавить стандартный список исключенных расширений.

4. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

- **SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

Параметр доступен, если снят флажок **Архивы**.

- **Упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

5. На закладке **Действия** выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Блокировать**

Kaspersky Security для Windows Server блокирует загрузку веб-страницы при обнаружении вредоносного содержимого. Вместо запрашиваемой веб-страницы отображается причина блокирования.

Kaspersky Security для Windows Server полностью удаляет зараженные вложения из сообщений электронной почты. Кроме того, в журнале выполнения задачи Защита трафика регистрируются события обнаружения угроз.

- **Разрешить**

Kaspersky Security для Windows Server не блокирует запрашиваемую веб-страницу. Вместо этого регистрируется событие обнаружения вредоносного содержимого.

Kaspersky Security для Windows Server не удаляет зараженные вложения из сообщений электронной почты. Однако в журнале выполнения задачи Защита трафика регистрируются события обнаружения угроз.

6. На закладке **Производительность** настройте следующие параметры:

- В разделе **Исключения** установите или снимите флажок **Не обнаруживать**. Чтобы настроить список исключенных объектов, выполните следующие действия:

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- a. Нажмите на кнопку **Изменить**.
- b. В открывшемся окне укажите имя объекта или маску.

с. Нажмите на кнопку **Добавить**.

- В разделе **Дополнительные параметры** ограничьте время проверки и размер объекта:

- **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстроедействие**.

- **Не проверять объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Kaspersky Security для Windows Server пропускает при антивирусной проверке объекты, размер которых превышает установленное ограничение.

Значение по умолчанию – 20 МБ.

7. Нажмите на кнопку **ОК** в окне **Параметры антивирусной защиты**.

Параметры уровня безопасности будут сохранены.

## Настройка защиты от почтовых угроз

Для использования защиты от почтовых угроз нужно установить расширение для Microsoft Outlook и правильно настроить устройство (см. раздел "Защита от почтовых угроз" на стр. [370](#)).

► Чтобы включить защиту от почтовых угроз, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).
2. На закладке **Защита от почтовых угроз** установите флажок **Включить защиту от почтовых угроз**.

Если установлен этот флажок, Kaspersky Security для Windows Server выполняет антивирусную и антифишинговую проверку всех входящих сообщений с помощью расширения Kaspersky Security для Microsoft Outlook.

Если флажок не установлен, электронная почта не проверяется.

По умолчанию флажок установлен.

При включении или выключении защиты от почтовых угроз изменения вступают в силу по истечении небольшого промежутка времени (5 минут) или сразу после перезапуска Microsoft Outlook.

3. Нажмите на кнопку **ОК**.

Изменения будут сохранены.

## Настройка обработки веб-адресов и веб-контента

► Чтобы проверять веб-ресурсы на наличие фишинга и обнаруживать вредоносные веб-адреса согласно антивирусной базе данных и репутации веб-адреса в KSN, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи **Защита трафика**" на стр. [378](#)).
2. На закладке **Общие** выберите и настройте режим работы задачи (см. раздел "Настройка режима работы задачи" на стр. [380](#)).
3. На закладке **Обработка веб-адресов и веб-контента** выполните следующие действия:

- Снимите или установите флажок **Использовать базу вредоносных веб-адресов для проверки веб-ссылок**.

Если флажок установлен, Kaspersky Security для Windows Server выполняет сигнатурный анализ каждого веб-адреса.

Если флажок снят, антивирусные базы не используются для проверки веб-адресов.

По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать антифишинговую базу для проверки веб-страниц**.

Если флажок установлен, Kaspersky Security для Windows Server проверяет каждый веб-адрес с помощью антифишинговой базы. Антифишинговая проверка основана на эвристическом анализе.

Если флажок снят, Kaspersky Security для Windows Server не обнаруживает фишинговые атаки.

По умолчанию флажок установлен.

Обратите внимание, что когда вы настраиваете антифишинговую проверку ссылок, антифишинг автоматически применяется и к электронным сообщениям.

- Снимите или установите флажок **Использовать доверенную зону**.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать KSN для защиты**.

Этот флажок включает или выключает использование служб KSN.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача не использует службы KSN.

По умолчанию флажок установлен.

Репутация веб-адресов в KSN доступна, только если выполнены все следующие условия:

- В параметрах задачи Защита трафика установлен флажок **Использовать KSN для защиты**.
- Принято Положение о KSN. Установлен флажок **Отправлять данные о запрашиваемых веб-адресах** (см. раздел **Настройка задачи Использование KSN с помощью Плагина управления** на стр. [353](#)).
- Задача Использование KSN запущена.

4. Нажмите на кнопку **ОК**.

Параметры обработки веб-адресов будут сохранены.

## Настройка веб-контроля

Настройте использование правил, управляйте параметрами проверки сертификатов и контролем веб-категорий.

### В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| Настройка проверки сертификатов .....            | <a href="#">389</a> |
| Настройка веб-контроля на основе категорий ..... | <a href="#">391</a> |
| Добавление правил для веб-адресов .....          | <a href="#">392</a> |

## Настройка проверки сертификатов

Kaspersky Security для Windows Server позволяет проверять и блокировать веб-ресурсы с недействительными сертификатами или сертификатами с истекшим сроком действия. Чтобы настроить проверку сертификатов, выполните следующие действия:

- а. Настройте задачу Защита трафика (см. раздел "Выбор и настройка режима работы задачи" на стр. [389](#)).
- б. Добавьте и примените Правила для сертификатов (см. раздел "Добавление правил для сертификатов" на стр. [390](#)).

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security для Windows Server создает только запрещающие правила для сертификатов.

### Выбор и настройка режима работы

► Чтобы выбрать и настроить режим работы с сертификатами, выполните следующие действия:

1. Откройте окно **Защита трафика** (см. раздел "Переход к параметрам политики для задачи Защита трафика" на стр. [378](#)).

2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим, поддерживающий проверку сертификатов:

- **Драйверный перехват** (см. раздел "Настройка режима Драйверный перехват" на стр. [380](#))
- **Перенаправление трафика** (см. раздел "Настройка режима Перенаправление трафика" на стр. [382](#))

3. В блоке **Параметры режима работы** настройте следующие параметры:

- **Проверять безопасные соединения по протоколу HTTPS**

Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:

- **TLS 1.0;**
- **TLS 1.1;**
- **TLS 1.2.**

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче **Защита трафика** только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

4. Нажмите на кнопку **ОК**.

Параметры задачи будут сохранены.

## Добавление правил для сертификатов

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security для Windows Server создает только запрещающие правила для сертификатов.

► *Чтобы добавить или настроить правило сертификата, выполните следующие действия:*

1. Откройте окно **Правила веб-контроля** (см. раздел "Переход к списку правил защиты трафика" на стр. [379](#)).
2. На закладке **Веб-контроль** установите флажок **Применять правила контроля сертификатов**.

Если флажок установлен, Kaspersky Security для Windows Server блокирует HTTPS-сертификаты с помощью пользовательских запрещающих правил для сертификатов.

Если флажок снят, программа не проверяется сертификаты.

По умолчанию флажок установлен.

3. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
4. В контекстном меню кнопки **Добавить** выберите пункт **Правило контроля сертификатов**.
5. В открывшемся окне **Правило контроля сертификатов** выполните следующие действия:
  - a. Введите название правила.
  - b. Установите флажок **Применять правило**.
  - c. Выберите **Тип оператора**: **Использовать маску** или **Использовать регулярные выражения**.
  - d. Укажите маску или регулярное выражение в поле **Оператор**.
  - e. Нажмите на кнопку **ОК**.
6. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
7. Нажмите на кнопку **Сохранить** в окне **Правила веб-контроля**.

Новые правила будут применены.

## Настройка веб-контроля на основе категорий

► Чтобы добавить или изменить правило защиты трафика на основе категорий, выполните следующие действия:

1. Откройте окно **Правила веб-контроля** (см. раздел "[Переход к списку правил защиты трафика](#)" на стр. [379](#)).
2. Выберите закладку **Категоризация**.
3. Установите флажок **Применять правила категоризации веб-ресурсов**.

Если флажок установлен, Kaspersky Security для Windows Server категоризирует и блокирует веб-ресурсы, попадающие в выбранные категории.

Если флажок снят, Kaspersky Security для Windows Server не выполняет категоризацию.

По умолчанию флажок снят.

Параметры контроля по веб-категориям становятся доступны.

4. Установите или снимите следующие флажки:
  - **Разрешать загрузку веб-страницы, если не удалось присвоить категорию**
  - **Разрешать загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда серверу**
  - **Разрешать загрузку легальных рекламных веб-ресурсов**
5. В списке доступных категорий (см. раздел "[Список категорий](#)" на стр. [371](#)):
  - Установите соответствующий флажок, чтобы разрешить категорию.  
Значение в графе **Тип правила** изменится на **Разрешающее**.
  - Снимите соответствующий флажок, чтобы запретить категорию.  
Значение в графе **Тип правила** изменится на **Запрещающее**.

Список категорий является стандартным, и его нельзя изменить (вы не можете добавлять или удалять категории).

6. Нажмите на кнопку **ОК**.

Параметры правил будут сохранены.

## Использование маски not-a-virus

- Чтобы использовать маску *not-a-virus* для анализа категорий, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте параметры задачи Использование KSN (см. раздел "Настройка задачи Использование KSN с помощью Плагина управления" на стр. [353](#)).
2. Установите флажок **Разрешить отправку данных о запрашиваемых веб-адресах**.
3. Запустите задачу Использование KSN.
4. В окне Параметры защиты трафика (см. раздел "Настройка задачи Защита трафика" на стр. [379](#)) установите флажок **Использовать KSN для защиты**.
5. В окне **Правила веб-контроля** на закладке **Категоризация** установите флажок **Применять правила категоризации веб-ресурсов**.
6. В списке категорий выберите категории, к которым вы хотите применить маску *not-a-virus*.  
Задача Защита трафика не будет обнаруживать объекты из выбранных категорий, которые соответствуют заданной маске.

Использование маски *not-a-virus* можно настроить в параметрах компонента Доверенная зона (см. раздел "Использование маски not-a-virus" на стр. [569](#)).

## Добавление правил для веб-адресов

Вы можете добавить правило контроля веб-адресов, чтобы запретить или разрешить конкретный веб-адрес. У правил самый высокий приоритет по сравнению с любыми другими заключениями.

- Чтобы создать новое правило контроля веб-адресов, выполните следующие действия:

1. Откройте окно **Правила веб-контроля** (см. раздел "Переход к списку правил защиты трафика" на стр. [379](#)).
2. На закладке **Веб-контроль** установите флажок **Применять правила контроля веб-адресов**.  
Если флажок установлен, Kaspersky Security для Windows Server блокирует веб-адреса с помощью пользовательских запрещающих правил для веб-адресов.  
Если флажок снят, программа не проверяется веб-адреса.  
По умолчанию флажок установлен.
3. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.



4. В контекстном меню кнопки **Добавить** выберите пункт **Контроль веб-адресов**.
  5. В открывшемся окне **Правило контроля веб-адресов** выполните следующие действия:
    - a. Введите название правила.
    - b. Выберите **Тип правила**: **Запрещающее** или **Разрешающее**.
    - c. Установите флажок **Применять правило**.
    - d. В поле **Веб-адрес** укажите веб-адрес.
    - e. Нажмите на кнопку **ОК**.
  6. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
  7. Нажмите на кнопку **ОК** в окне **Правила веб-контроля**.
- Новые правила будут применены.

## Управление защитой трафика с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

### В этом разделе

|                                                      |                     |
|------------------------------------------------------|---------------------|
| Навигация .....                                      | <a href="#">393</a> |
| Настройка задачи Защита трафика .....                | <a href="#">394</a> |
| Настройка антивирусной защиты .....                  | <a href="#">399</a> |
| Настройка защиты от почтовых угроз .....             | <a href="#">402</a> |
| Настройка обработки веб-адресов и веб-контента ..... | <a href="#">403</a> |
| Настройка веб-контроля .....                         | <a href="#">404</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| Переход к параметрам задачи Защита трафика ..... | <a href="#">394</a> |
| Переход к окну Правила защиты трафика .....      | <a href="#">394</a> |

## Переход к параметрам задачи Защита трафика

- Чтобы перейти к общим параметрам задачи Защита трафика в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

## Переход к окну Правила защиты трафика

- Чтобы перейти к списку правил защиты трафика в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита трафика**.
3. В панели результатов узла **Защита трафика** перейдите по ссылке **Правила веб-контроля**.

Откроется окно **Правила веб-контроля**.

Настройте список правил в соответствии с вашими требованиями.

## Настройка задачи Защита трафика

- Чтобы настроить задачу Защита трафика, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Общие** выберите и настройте режим работы задачи (см. раздел "Настройка режима работы задачи" на стр. [395](#)).
3. На закладке **Обработка веб-адресов и веб-контента** настройте антифишинговую и антивирусную проверку веб-адресов (см. раздел "Настройка режима Драйверный перехват" на стр. [395](#)).
4. На закладке **Антивирусная защита** настройте эвристический анализ и уровень безопасности (см. раздел "Настройка антивирусной защиты" на стр. [399](#)).
5. На закладках **Расписание** и **Дополнительно** настройте запуск задачи в соответствии с расписанием (см. раздел "Работа с расписанием задач" на стр. [141](#)).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

### В этом разделе

|                                                |                     |
|------------------------------------------------|---------------------|
| Настройка режима работы задачи .....           | <a href="#">395</a> |
| Настройка режима Драйверный перехват .....     | <a href="#">395</a> |
| Настройка режима Перенаправление трафика ..... | <a href="#">397</a> |

## Настройка режима работы задачи

► Чтобы настроить режим работы задачи, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Общие** выберите один из доступных режимов в раскрывающемся списке **Режим работы задачи**:
  - **Драйверный перехват**
  - **Перенаправление трафика**
  - **Внешний прокси-сервер**
3. Укажите **параметры соединения с ICAP-сервисом** (требуется для всех трех режимов):
  - **Номер сетевого порта**  
Номер порта ICAP службы Kaspersky Security для Windows Server.
  - **Идентификатор службы**  
Идентификатор, который является частью параметра RESPMOD URI протокола ICAP (см. документ RFC 3507). RESPMOD URI обозначает адрес антивирусного ICAP-сервера, установленный для сетевого хранилища.  
  
Например, если IP-адрес защищаемого устройства – 192.168.10.10, номер порта – 1345, а идентификатор ICAP-службы – webscan, эти параметры соответствуют следующему адресу RESPMOD URI – icap://192.168.10.10/webscan:1345.

Перезапустите задачу, чтобы применить параметры подключения ICAP-службы.

4. Настройте выбранный режим работы задачи.

Для режима **Внешний прокси-сервер** дополнительная настройка не требуется. Настройка выполняется на стороне внешнего прокси-сервера.

5. Нажмите на кнопку **ОК**.  
Параметры будут сохранены.

## Настройка режима Драйверный перехват

► Чтобы настроить режим **Драйверный перехват**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Общие** выберите режим **Драйверный перехват**.
3. В блоке **Параметры режима работы** настройте следующие параметры:
  - **Проверять безопасные соединения по протоколу HTTPS**  
Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:

- **TLS 1.0;**
- **TLS 1.1;**
- **TLS 1.2.**

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче **Защита трафика** только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

- **Не доверять веб-серверам с недействительными сертификатами**

Этот флажок доступен, только если установлен флажок **Проверять безопасные соединения по протоколу HTTPS**.

Если этот флажок установлен, веб-страница с недействительным сертификатом блокируется (например, если закончился срок действия сертификата, возникла ошибка проверки подписи, сертификат отозван и т. д.).

- **Порт безопасности**

Укажите номер порта, используемого для перенаправления трафика из браузера или сетевого драйвера на внутренний порт Kaspersky Security для Windows Server для обнаружения веб-угроз. Не рекомендуется изменять порт, указанный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если используется режим **Перенаправление трафика**, используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.

4. Чтобы добавить порты в область перехвата или исключить из нее, нажмите на кнопку **Настроить область перехвата**.

Откроется окно **Область перехвата**.

5. На закладке **Перехватывать по портам** выберите один из следующих вариантов:

- **Перехватывать все**
- **Перехватывать по указанным портам**

- a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.

- b. Нажмите на кнопку **Добавить**.

Порт будет включен в область перехвата.

По умолчанию Kaspersky Security для Windows Server перехватывает трафик, передаваемый через следующие порты: 80, 8080, 3128, 443.

6. Чтобы указать порты, которые требуется исключить из области перехвата, на закладке **Исключить порты** выполните следующие действия:
  - a. Введите номер порта в текстовое поле. Можно добавить несколько номеров портов через точку с запятой.
  - b. Нажмите на кнопку **Добавить**.

Порт будет исключен из области перехвата.

По умолчанию Kaspersky Security для Windows Server исключает порты, которые используются другими программами и могут вызывать проблемы при попытке просмотра содержимого, передаваемого по зашифрованному соединению: 3389, 1723, 13291.

7. Чтобы исключить IP-адреса из области перехвата, на закладке **Исключить IP-адреса** выполните следующие действия:
    - a. Введите IP-адрес в формате IPv4 (в краткой форме или указав адрес с помощью маски подсети).
    - b. Нажмите на кнопку **Добавить**.
    - c. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
  8. Чтобы исключить процесс или исполняемый файл, который требует обмена трафиком, на закладке **Исключить процессы** выполните следующие действия:
    - a. Установите флажок **Применять исключения для процессов**.
    - b. Чтобы исключить файл, выполните следующие действия:
      1. Нажмите на кнопку **Исполняемые файлы**.  
Отобразится стандартное окно **Открыть**.
      2. Выберите исполняемый файл, который хотите исключить, и нажмите **Открыть**.
  9. В окне **Область перехвата** нажмите на кнопку **ОК**.
  10. В окне **Параметры задачи** нажмите на кнопку **ОК**.
- Параметры режима работы задачи будут сохранены.

## Настройка режима Перенаправление трафика

► Чтобы настроить режим *Перенаправление трафика*, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Общие** выберите режим **Перенаправление трафика**.
3. В блоке **Параметры режима работы** настройте следующие параметры:
  - **Проверять безопасные соединения по протоколу HTTPS**

Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:
  - TLS 1.0;
  - TLS 1.1;
  - TLS 1.2.

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче Защита трафика только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

- **Порт безопасности**

Укажите номер порта, используемого для перенаправления трафика из браузера или сетевого драйвера на внутренний порт Kaspersky Security для Windows Server для обнаружения веб-угроз. Не рекомендуется изменять порт, указанный по умолчанию. Номер порта не должен совпадать с портами, открытыми для службы ICAP. Если используется режим **Перенаправление трафика**, используемые порты перечислены в поле **Проверять безопасные соединения по протоколу HTTPS**.

- **Перенаправлять трафик на внешний прокси-сервер после проверки**

Если флажок установлен, Kaspersky Security для Windows Server перенаправляет уже проверенный трафик на внешний прокси-сервер, например, на корпоративный прокси-сервер, используемый в сети организации.

Если флажок снят, трафик направляется на внутренний прокси-сервер.

- **Адрес прокси-сервера**

Адрес внутреннего терминального прокси-сервера для перенаправления трафика. Введите адрес в формате IPv4.

- **Порт**

Номер порта для внутреннего прокси-сервера.

Для режима **Перенаправление трафика** в операционной системе должно быть настроено перенаправление зашифрованного трафика через порт, указанный в Kaspersky Security для Windows Server.

4. Нажмите на кнопку **ОК**.

Параметры режима работы задачи будут сохранены.

## Настройка антивирусной защиты

Следующие параметры защиты влияют на весь входящий трафик. Однако выбранные действия над зараженными и прочими обнаруженными объектами выполняются только для почтовых вложений. Задача Защита трафика передает в Kaspersky Sandbox только файлы документов.

► Чтобы настроить эвристический анализ для обнаружения вирусов и других угроз компьютерной безопасности, передаваемых через веб-трафик, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Антивирусная защита** выполните следующие действия:
  - Установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

- Установите флажок **Использовать эвристический анализатор**.
  - Выберите нужный уровень эвристического анализа для антивирусной проверки.
  - Выберите уровень защиты (см. раздел "Параметры стандартных уровней безопасности" на стр. [375](#)) из раскрывающегося списка:
    - **Рекомендуемый**
    - **Максимальная защита**
    - **Максимальное быстродействие**
    - **Пользовательский**
3. На закладке **Описание** вы можете просмотреть параметры выбранного уровня безопасности.
  4. На закладке **Общие** в разделе **Защита объектов** укажите объекты, которые вы хотите включить в область проверки:
    - **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- а. Нажмите на кнопку **Изменить**, чтобы изменить список расширений.
- б. В открывшемся окне укажите расширение.
- с. Нажмите на кнопку **Добавить**.

Нажмите на кнопку **По умолчанию**, чтобы добавить стандартный список исключенных расширений.

5. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

- **SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

Параметр доступен, если снят флажок **Архивы**.

- **Упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками



двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

6. На закладке **Действия** выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Блокировать**

Kaspersky Security для Windows Server блокирует загрузку веб-страницы при обнаружении вредоносного содержимого. Вместо запрашиваемой веб-страницы отображается причина блокирования.

Kaspersky Security для Windows Server полностью удаляет зараженные вложения из сообщений электронной почты. Кроме того, в журнале выполнения задачи Защита трафика регистрируются события обнаружения угроз.

- **Разрешить**

Kaspersky Security для Windows Server не блокирует запрашиваемую веб-страницу. Вместо этого регистрируется событие обнаружения вредоносного содержимого.

Kaspersky Security для Windows Server не удаляет зараженные вложения из сообщений электронной почты. Однако в журнале выполнения задачи Защита трафика регистрируются события обнаружения угроз.

7. На закладке **Производительность** настройте следующие параметры:

- В разделе **Исключения** установите или снимите флажок **Не обнаруживать**. Чтобы настроить список исключенных объектов, выполните следующие действия:

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- а. Нажмите на кнопку **Изменить**.

- b. В открывшемся окне укажите имя объекта или маску.
  - c. Нажмите на кнопку **Добавить**.
  - В разделе **Дополнительные параметры** ограничьте время проверки и размер объекта:
    - **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
    - **Не проверять объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Kaspersky Security для Windows Server пропускает при антивирусной проверке объекты, размер которых превышает установленное ограничение.

Значение по умолчанию – 20 МБ.
8. В окне **Параметры задачи** нажмите на кнопку **ОК**.
- Параметры уровня защиты будут сохранены.

## Настройка защиты от почтовых угроз

► Чтобы включить защиту от почтовых угроз, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Защита трафика**" на стр. [394](#)).
2. На закладке **Защита от почтовых угроз** установите флажок **Включить защиту от почтовых угроз**.

Если установлен этот флажок, Kaspersky Security для Windows Server выполняет антивирусную и антифишинговую проверку всех входящих сообщений с помощью расширения Kaspersky Security для Microsoft Outlook.

Если флажок не установлен, электронная почта не проверяется.

По умолчанию флажок установлен.

При включении или выключении защиты от почтовых угроз изменения вступают в силу по истечении небольшого промежутка времени (5 минут) или сразу после перезапуска Microsoft Outlook.

3. Нажмите на кнопку **ОК**.
- Изменения будут сохранены.

## Настройка обработки веб-адресов и веб-контента

Чтобы проверять веб-ресурсы на наличие фишинга и обнаруживать вредоносные веб-адреса согласно антивирусной базе данных и репутации веб-адреса в KSN, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи **Защита трафика**" на стр. [394](#)).
2. На закладке **Общие** в разделе **Режим работы задачи** выберите и настройте режим работы задачи (см. раздел "Настройка режима работы задачи" на стр. [395](#)).
3. На закладке **Обработка веб-адресов и веб-контента** выполните следующие действия:

- Снимите или установите флажок **Использовать базу вредоносных веб-адресов для проверки веб-ссылок**.

Если флажок установлен, Kaspersky Security для Windows Server выполняет сигнатурный анализ каждого веб-адреса.

Если флажок снят, антивирусные базы не используются для проверки веб-адресов.

По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать антифишинговую базу для проверки веб-страниц**.

Если флажок установлен, Kaspersky Security для Windows Server проверяет каждый веб-адрес с помощью антифишинговой базы. Антифишинговая проверка основана на эвристическом анализе.

Если флажок снят, Kaspersky Security для Windows Server не обнаруживает фишинговые атаки.

По умолчанию флажок установлен.

Обратите внимание, что когда вы настраиваете антифишинговую проверку ссылок, антифишинг автоматически применяется и к электронным сообщениям.

- Снимите или установите флажок **Использовать доверенную зону**.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать KSN для защиты**.

Этот флажок включает или выключает использование служб KSN.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача не использует службы KSN.

По умолчанию флажок установлен.

Репутация веб-адресов в KSN доступна, только если выполнены все следующие условия:

- В параметрах задачи Защита трафика установлен флажок **Использовать KSN для защиты**.
- Принято Положение о KSN. Установлен флажок **Разрешить отправку данных о проверяемых веб-адресах** (см. раздел **Настройка параметров задачи Использование KSN с помощью Консоли программы** на стр. [358](#)).
- Задача Использование KSN запущена.

4. Нажмите на кнопку **ОК**.

Параметры обработки веб-адресов будут сохранены.

## Настройка веб-контроля

Настройте использование правил, управляйте параметрами проверки сертификатов и контролем веб-категорий.

### В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| Настройка проверки сертификатов .....            | <a href="#">404</a> |
| Настройка веб-контроля на основе категорий ..... | <a href="#">406</a> |
| Добавление правил для веб-адресов .....          | <a href="#">407</a> |

## Настройка проверки сертификатов

Kaspersky Security для Windows Server позволяет проверять и блокировать веб-ресурсы с недействительными сертификатами или сертификатами с истекшим сроком действия. Чтобы настроить проверку сертификатов, выполните следующие действия:

- а. Настройте задачу Защита трафика (см. раздел "Выбор и настройка режима работы задачи" на стр. [404](#)).
- б. Добавьте и примените Правила для сертификатов (см. раздел "Добавление правил для сертификатов" на стр. [405](#)).

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security для Windows Server создает только запрещающие правила для сертификатов.

### Выбор и настройка режима работы

Чтобы выбрать и настроить режим работы с сертификатами, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Защита трафика" на стр. [394](#)).
2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим, поддерживающий проверку сертификатов:
  - **Драйверный перехват** (см. раздел "Настройка режима Драйверный перехват" на стр. [395](#))
  - **Перенаправление трафика**

3. В блоке **Параметры режима работы** настройте следующие параметры:

- **Проверять безопасные соединения по протоколу HTTPS**

Если флажок установлен, программа распаковывает перехваченный HTTPS-трафик и проверяет на наличие угроз.

Если флажок снят, программа не распаковывает зашифрованный HTTPS-трафик.

По умолчанию флажок установлен.

Проверка доступна, только если открыт HTTPS-порт.

- Выберите версии протокола шифрования, которые вы хотите использовать:

- **TLS 1.0;**
- **TLS 1.1;**
- **TLS 1.2.**

По умолчанию выбраны все версии. При этом выбор варианта **TLS 1.0** отменить невозможно.

Обратите внимание, что протокол TLS можно использовать в задаче Защита трафика только на защищаемых устройствах с операционной системой Microsoft Windows 7 и выше или Microsoft Windows Server 2008 R2 и выше.

4. Нажмите на кнопку **ОК**.

Параметры задачи будут сохранены.

## Добавление правил для сертификатов

Правила для сертификатов можно использовать только в режиме работы **Драйверный перехват** или **Перенаправление трафика**. По умолчанию Kaspersky Security для Windows Server создает только запрещающие правила для сертификатов.

► Чтобы добавить или настроить правило сертификата, выполните следующие действия:

1. Откройте окно **Правила веб-контроля** (см. раздел "Переход к окну Правила защиты трафика" на стр. [394](#)).
2. На закладке **Веб-контроль** установите флажок **Применять правила контроля сертификатов**.  
Если флажок установлен, Kaspersky Security для Windows Server блокирует HTTPS-сертификаты с помощью пользовательских запрещающих правил для сертификатов.  
Если флажок снят, программа не проверяется сертификаты.  
По умолчанию флажок установлен.
3. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
4. В контекстном меню кнопки **Добавить** выберите пункт **Правило контроля сертификатов**.
5. В открывшемся окне **Правило контроля сертификатов** выполните следующие действия:

- a. Введите название правила.
  - b. Установите флажок **Применять правило**.
  - c. Выберите **Тип оператора**: **Использовать маску** или **Использовать регулярные выражения**.
  - d. Укажите маску или регулярное выражение в поле **Оператор**.
  - e. Нажмите на кнопку **ОК**.
6. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
  7. Нажмите на кнопку **Сохранить** в окне **Правила веб-контроля**.

Новые правила будут применены.

## Настройка веб-контроля на основе категорий

► Чтобы добавить или изменить правило защиты трафика на основе категорий, выполните следующие действия:

1. Откройте окно **Правила веб-контроля** (см. раздел "Переход к окну Правила защиты трафика" на стр. [394](#)).
2. Выберите закладку **Категоризация**.
3. Установите флажок **Применять правила категоризации веб-ресурсов**.

Если флажок установлен, Kaspersky Security для Windows Server категоризирует и блокирует веб-ресурсы, попадающие в выбранные категории.

Если флажок снят, Kaspersky Security для Windows Server не выполняет категоризацию.

По умолчанию флажок снят.

Параметры контроля по веб-категориям становятся доступны.

4. Установите или снимите следующие флажки:
  - **Разрешать загрузку веб-страницы, если не удалось присвоить категорию**
  - **Разрешать загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда серверу**
  - **Разрешать загрузку легальных рекламных веб-ресурсов**
5. В списке доступных категорий (см. раздел "Список категорий" на стр. [371](#)):
  - Установите соответствующий флажок, чтобы разрешить категорию.  
Значение в графе **Тип** изменится на **Разрешающее**.
  - Снимите соответствующий флажок, чтобы запретить категорию.  
Значение в графе **Тип** изменится на **Запрещающее**.

Список категорий является стандартным, и его нельзя изменить (вы не можете добавлять или удалять категории).

6. Нажмите на кнопку **Сохранить**.

Параметры правил будут сохранены.

## Использование маски not-a-virus

► Чтобы использовать маску *not-a-virus* для анализа категорий, выполните следующие действия:

1. В дереве Консоли программы перейдите к параметрам задачи Использование KSN (см. раздел "Настройка задачи Использование KSN с помощью Консоли программы" на стр. [358](#)).
2. Установите флажок **Разрешить отправку данных о проверяемых веб-адресах**.
3. Запустите задачу Использование KSN.
4. В окне Параметры защиты трафика (см. раздел "Настройка режима Драйверный перехват" на стр. [395](#)) установите флажок **Использовать KSN для защиты**.
5. В окне **Правила веб-контроля** на закладке **Категоризация** установите флажок **Применять правила категоризации веб-ресурсов**.
6. В списке категорий выберите категории, к которым вы хотите применить маску *not-a-virus*.

Задача Защита трафика не будет обнаруживать объекты из выбранных категорий, которые соответствуют заданной маске.

Использование маски *not-a-virus* можно настроить в параметрах компонента Доверенная зона (см. раздел "Использование маски *not-a-virus*" на стр. [575](#)).

## Добавление правил для веб-адресов

Вы можете добавить правило контроля веб-адресов, чтобы запретить или разрешить конкретный веб-адрес. У правил самый высокий приоритет по сравнению с любыми другими заключениями.

► Чтобы создать новое правило контроля веб-адресов, выполните следующие действия:

1. Откройте окно **Правила веб-контроля** (см. раздел "Переход к окну Правила защиты трафика" на стр. [394](#)).
2. На закладке **Веб-контроль** установите флажок **Применять правила контроля веб-адресов**.

Если флажок установлен, Kaspersky Security для Windows Server блокирует веб-адреса с помощью пользовательских запрещающих правил для веб-адресов.

Если флажок снят, программа не проверяется веб-адреса.

По умолчанию флажок установлен.

3. Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
4. В контекстном меню кнопки **Добавить** выберите пункт **Контроль веб-адресов**.
5. В открывшемся окне **Правило контроля веб-адресов** выполните следующие действия:
  - a. Введите название правила.
  - b. Выберите **Тип правила**: **Запрещающее** или **Разрешающее**.
  - c. Установите флажок **Применять правило**.
  - d. В поле **Веб-адрес** укажите веб-адрес.

- е. Нажмите на кнопку **ОК**.
6. Чтобы изменить правило, выберите нужное правило из списка и нажмите на кнопку **Изменить**.
7. Нажмите на кнопку **Сохранить** в окне **Правила веб-контроля**.
- Новые правила будут применены.

## Управление защитой трафика с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров задачи на защищаемом устройстве.

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита трафика**.
6. Настройте параметры, приведены в следующей таблице.

Table 68. Параметры задачи Защита трафика

Table 69.

| Закладка                                    | Описание                                                                                                                                                                     |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Общие</b>                                | Можно выбирать и настраивать режим работы задачи (см. раздел "Настройка режима работы задачи" на стр. <a href="#">380</a> ).                                                 |
| <b>Режим защиты</b>                         | Можно настраивать эвристический анализатор и уровень безопасности (см. раздел "Настройка антивирусной защиты" на стр. <a href="#">384</a> ).                                 |
| <b>Обработка веб-адресов и веб-контента</b> | Можно настраивать антифишинговую и антивирусную проверку веб-адресов (см. раздел "Настройка обработки веб-адресов и веб-контента" на стр. <a href="#">388</a> ).             |
| <b>Веб-контроль</b>                         | Можно настроить правила и управлять параметрами проверки сертификатов и веб-контроля на основе категорий (см. раздел "Настройка веб-контроля" на стр. <a href="#">389</a> ). |
| <b>Категоризация</b>                        | Можно добавить или изменить правило защиты трафика на основе категорий (см. раздел "Настройка веб-контроля на основе категорий" на стр. <a href="#">391</a> ).               |
| <b>Управление задачами</b>                  | Вы можете настроить расписание запуска задачи.                                                                                                                               |



# Защита от шифрования

Этот раздел содержит информацию о задаче Защита от шифрования и инструкции по настройке ее параметров.

## В этом разделе

|                                                                          |                     |
|--------------------------------------------------------------------------|---------------------|
| О задаче Защита от шифрования .....                                      | <a href="#">409</a> |
| Статистика задачи Защита от шифрования .....                             | <a href="#">410</a> |
| Параметры по умолчанию для задачи Защита от шифрования .....             | <a href="#">411</a> |
| Настройка задачи Защита от шифрования с помощью Плагина управления ..... | <a href="#">411</a> |
| Настройка задачи Защита от шифрования с помощью Консоли программы .....  | <a href="#">416</a> |
| Настройка задачи Защита от шифрования с помощью Веб-плагина .....        | <a href="#">420</a> |

## О задаче Защита от шифрования

Задача Защита от шифрования позволяет обнаруживать вредоносное шифрование сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств в сети организации.

В ходе выполнения задачи Защита от шифрования, Kaspersky Security для Windows Server проверяет обращения удаленных устройств к файлам, расположенным в папках общего доступа на защищаемом устройстве. Если программа расценивает действия удаленного устройства над сетевыми файловыми ресурсами как вредоносное шифрование, то Kaspersky Security для Windows Server вносит локально уникальный идентификатор (LUID) этого устройства в список заблокированных узлов.

Задача Защита от шифрования может выполняться в синхронном и асинхронном режиме. По умолчанию, задача Защита от шифрования работает в асинхронном режиме. Обработка файловых операций распределяется на несколько параллельных потоков. Дополнительная информация о синхронном и асинхронном режиме обработки файловых операций и об изменении режима обработки файловых операций приведена в базе знаний "Лаборатории Касперского" (см. раздел "Источники для самостоятельного поиска информации" на стр. [18](#)).

Kaspersky Security для Windows Server не расценивает активность шифрования как вредоносную, если обнаруженная активность шифрования ведется в папках, исключенных из области действия задачи Защита от шифрования.

По умолчанию программа блокирует доступ к сетевым файловым ресурсам на 30 минут.

**Задача Защита от шифрования не блокирует доступ со стороны узла к сетевым файловым ресурсам до тех пор, пока активность этого узла не признана вредоносной. Это может занять некоторое время, в течение которого программа-шифровальщик может вести вредоносную активность.**

Если задача Защита от шифрования запущена в режиме Только статистика, Kaspersky Security для Windows Server только регистрирует попытки вредоносного шифрования со стороны удаленных устройств в журнале выполнения задачи.

## Статистика задачи Защита от шифрования

Когда выполняется задача Защита от шифрования, можно просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Security для Windows Server с момента запуска задачи, то есть статистику выполнения задачи.

► Чтобы просмотреть статистику задачи Защита от шифрования, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита от шифрования**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Security для Windows Server обработала за время выполнения задачи (см. таблицу ниже).

Table 70. Статистика задачи Защита от шифрования

| Поле                                              | Описание                                                                                                                |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Обнаружены попытки вредоносного шифрования</b> | Количество попыток доступа, в которых программа Kaspersky Security для Windows Server обнаружила активность шифрования. |
| <b>Ошибок обработки</b>                           | Количество обращений программ к области хранения, вызвавших ошибку задачи.                                              |
| <b>Обработано объектов</b>                        | Общее количество обращений, обработанных Kaspersky Security для Windows Server.                                         |

## Параметры по умолчанию для задачи Защита от шифрования

По умолчанию в задаче Защита от шифрования используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 71. Параметры по умолчанию для задачи Защита от шифрования

| Параметр                        | Значение по умолчанию                                                                                                                                            | Описание                                                                                                             |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Режим работы</b>             | Активный                                                                                                                                                         | Задача Защита от шифрования может быть запущена в режиме <b>Активный</b> или <b>Только уведомлять</b> .              |
| <b>Область защиты</b>           | По умолчанию Kaspersky Security для Windows Server применяет задачу Защита от шифрования ко всем папкам общего доступа защищаемого устройства.                   | Вы можете изменить область защиты, указав папки общего доступа, к которым должна применяться задача.                 |
| <b>Исключения</b>               | Применяется список исключений, который включает элементы, добавленные специалистами "Лаборатории Касперского".                                                   | Укажите области, которые вы хотите исключить из области защиты.                                                      |
| <b>Эвристический анализатор</b> | Эвристический анализатор включен, и в Kaspersky Security для Windows Server применяется <b>Средний</b> уровень глубины проверки.                                 | Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень глубины проверки. |
| <b>Параметры расписания</b>     | По умолчанию время первого запуска задачи не задано. Задача Защита от шифрования не запускается автоматически при запуске Kaspersky Security для Windows Server. | Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень глубины проверки. |



## Настройка задачи Защита от шифрования с помощью Плагина управления

► Чтобы настроить параметры задачи Защита от шифрования, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

5. В открывшемся окне настройте следующие параметры:
  - Режим работы задачи и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. [412](#)) на закладке **Общие**.
  - Область защиты (см. раздел "Формирование области защиты" на стр. [414](#)) на закладке **Область защиты**.
  - Исключения (см. раздел "Добавление исключений" на стр. [415](#)) на закладке **Исключения**.
  - Запуск задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. [141](#)) на закладке **Управление задачами**.
6. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

|                                   |                     |
|-----------------------------------|---------------------|
| Общие параметры задачи.....       | <a href="#">412</a> |
| Формирование области защиты ..... | <a href="#">414</a> |
| Добавление исключений .....       | <a href="#">415</a> |

## Общие параметры задачи

► *Чтобы настроить общие параметры задачи, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

5. В разделе **Режим работы** на закладке **Общие** выберите режим **Активный**.

Если выбран этот режим, Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа для скомпрометированных устройств при обнаружении попытки вредоносного шифрования.

6. Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

7. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".  
Этот уровень выбран по умолчанию.
- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

8. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

## Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная.** Можно использовать область защиты, заданную по умолчанию и включающую все папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки сервера**.
- **Пользовательская.** Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные папки общего доступа**.

Для настройки области защиты задачи Защита от шифрования можно использовать только локальный путь.

► Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

5. На закладке **Область защиты** выберите папки, которые Kaspersky Security для Windows Server будет проверять в ходе выполнения задачи Защита от шифрования:

- **Все сетевые папки общего доступа сервера**

Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security для Windows Server проверяет все папки общего доступа на защищаемом устройстве.

Этот вариант выбран по умолчанию.

- **Только указанные папки общего доступа**

Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security для Windows Server обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.

6. Чтобы указать папки общего доступа на устройстве, которые вы хотите включить в область защиты от шифрования, выполните следующие действия:
  - a. Выберите вариант **Только указанные папки общего доступа** и нажмите на кнопку **Добавить**.  
Откроется окно **Выберите папку для добавления**.
  - b. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.
  - c. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Защита от шифрования**.  
Настроенные параметры будут сохранены.

## Добавление исключений

► *Чтобы добавить исключения из области защиты от шифрования, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.  
Откроется окно **Защита от шифрования**.
5. На закладке **Исключения** установите флажок **Применить список исключений**.

Если флажок установлен, то во время выполнения задачи Защита от шифрования Kaspersky Security для Windows Server не обнаруживает вредоносное шифрование в указанных областях.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает попытки

шифрования во всех папках общего доступа.

По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

- \*.stt;
- \*.sig;
- \*.exe;
- \*.sldprt.

6. Нажмите на кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.

7. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.

8. Нажмите на кнопку **ОК**.

Исключенная область будет добавлена в список.

## Настройка задачи Защита от шифрования с помощью Консоли программы

- Чтобы настроить параметры задачи Защита от шифрования, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне настройте следующие параметры:
  - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. [417](#)) на закладке **Общие**.
  - Область защиты (см. раздел "Формирование области защиты" на стр. [418](#)) на закладке **Область защиты**.
  - Исключения (см. раздел "Добавление исключений" на стр. [419](#)) на закладке **Исключения**.
  - Запуск задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. [141](#)) на закладках **Расписание** и **Дополнительно**.
5. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.



## В этом разделе

|                                   |                     |
|-----------------------------------|---------------------|
| Общие параметры задачи.....       | <a href="#">417</a> |
| Формирование области защиты ..... | <a href="#">418</a> |
| Добавление исключений .....       | <a href="#">419</a> |

## Общие параметры задачи

► Чтобы настроить общие параметры задачи, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В разделе **Режим работы** на закладке **Общие** выберите режим **Активный**.

Если выбран этот режим, Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа для скомпрометированных устройств при обнаружении попытки вредоносного шифрования.

5. Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

6. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных

срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

7. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

## Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная.** Можно использовать область защиты, заданную по умолчанию и включающую в проверку все сетевые папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки сервера**.
- **Пользовательская.** Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные папки общего доступа**.

Для настройки области защиты задачи Защита от шифрования можно использовать только локальный путь.

При использовании стандартной или пользовательской области защиты можно исключить выбранные папки из области защиты, например, если данные в этих папках шифруются программами, установленными на удаленных устройствах.

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладке **Область защиты** выберите папки, которые Kaspersky Security для Windows Server будет проверять в ходе выполнения задачи Защита от шифрования:
  - **Все сетевые папки общего доступа сервера**  
Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security для Windows Server проверяет все папки общего доступа на защищаемом устройстве.  
Этот вариант выбран по умолчанию.
  - **Только указанные папки общего доступа**  
Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security для Windows Server обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.
5. Чтобы указать папки общего доступа на защищаемом устройстве, которые вы хотите включить в область защиты от шифрования, используйте один из следующих способов:

- Вручную:
  - a. Введите имя папки общего доступа на защищаемом устройстве.
  - b. Нажмите на кнопку **Добавить**.  
Папка будет добавлена в список.
- Выбор папки:
  - a. Нажмите на кнопку **Обзор**.  
Откроется стандартное окно Microsoft Windows.
  - b. Выберите папку, которую вы хотите добавить в область защиты задачи.
  - c. Нажмите на кнопку **ОК**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Добавление исключений

► Чтобы настроить область защиты для задачи *Защита от шифрования*, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита сервера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Применить список исключений**.

Если флажок установлен, то во время выполнения задачи *Защита от шифрования* Kaspersky Security для Windows Server не обнаруживает вредоносное шифрование в указанных областях.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает попытки шифрования во всех папках общего доступа.

По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

- \*.stt;
- \*.sig;
- \*.exe;
- \*.sldprt.

5. Укажите название или маску названия папки.
6. Нажмите на кнопку **Добавить**.
7. При необходимости повторите шаги 5 и 6 для добавления исключений.
8. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Исключения из области защиты будут добавлены и применены.

## Настройка задачи Защита от шифрования с помощью Веб-плагина

В этом разделе описано управление задачей Защита от шифрования с помощью интерфейса Веб-плагина.

### В этом разделе

|                                   |                     |
|-----------------------------------|---------------------|
| Общие параметры задачи.....       | <a href="#">420</a> |
| Формирование области защиты ..... | <a href="#">421</a> |
| Добавление исключений .....       | <a href="#">422</a> |

## Общие параметры задачи

► Чтобы настроить общие параметры задачи, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.
6. На закладке **Общие** выберите режим **Активный**.

Если выбран этот режим, Kaspersky Security для Windows Server блокирует доступ к папкам общего доступа для скомпрометированных устройств при обнаружении попытки вредоносного шифрования.

7. В разделе **Эвристический анализатор** выполните одно из следующих действий:

- Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

- Если требуется, отрегулируйте уровень эвристического анализа.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и

выполняется быстрее.

- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

8. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

## Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная.** Можно использовать область защиты, заданную по умолчанию и включающую в проверку все сетевые папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки сервера**.
- **Пользовательская.** Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные папки общего доступа**.

Для настройки области защиты задачи Защита от шифрования можно использовать только локальный путь.

При использовании стандартной или пользовательской области защиты можно исключить выбранные папки из области защиты, например, если данные в этих папках шифруются программами, установленными на удаленных устройствах.

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.
6. На закладке **Область защиты** выберите папки, которые Kaspersky Security для Windows Server будет проверять в ходе выполнения задачи Защита от шифрования:
  - **Все сетевые папки общего доступа сервера**

Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования

Kaspersky Security для Windows Server проверяет все папки общего доступа на защищаемом устройстве.

Этот вариант выбран по умолчанию.

- **Только указанные папки общего доступа**

Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Security для Windows Server обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.

7. Чтобы указать папки общего доступа на устройстве, которые вы хотите включить в область защиты от шифрования, выполните следующие действия:
  - a. Выберите вариант **Только указанные папки общего доступа** и нажмите на кнопку **Добавить**.
  - b. На панели справа укажите путь к папке.
  - c. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

Настроенные параметры будут сохранены.

## Добавление исключений

► *Чтобы настроить параметры задачи Защита от шифрования, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.
6. На закладке **Список исключений** установите флажок **Применить список исключений**.

Если флажок установлен, то во время выполнения задачи Защита от шифрования Kaspersky Security для Windows Server не обнаруживает вредоносное шифрование в указанных областях.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает попытки шифрования во всех папках общего доступа.

По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

- \*.stt;
- \*.sig;
- \*.exe;
- \*.sldprt.

7. Нажмите на кнопку **Добавить**.
8. На панели справа укажите путь к папке или маску.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

Исключения из области защиты будут добавлены и применены.

# Контроль запуска программ

Этот раздел содержит информацию о задаче Контроль запуска программ и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| О задаче Контроль запуска программ .....                                | <a href="#">424</a> |
| О правилах контроля запуска программ .....                              | <a href="#">425</a> |
| О Контроле пакетов установки .....                                      | <a href="#">427</a> |
| Об использовании KSN в задаче Контроль запуска программ .....           | <a href="#">430</a> |
| О формировании правил контроля запуска программ .....                   | <a href="#">431</a> |
| Параметры по умолчанию для задачи Контроль запуска программ.....        | <a href="#">433</a> |
| Управление контролем запуска программ с помощью Плагина управления..... | <a href="#">436</a> |
| Управление контролем запуска программ с помощью Консоли программы.....  | <a href="#">460</a> |
| Управление контролем запуска программ с помощью веб-плагина .....       | <a href="#">478</a> |

## О задаче Контроль запуска программ

Во время выполнения задачи Контроль запуска программ Kaspersky Security для Windows Server проверяет попытки пользователей запускать различные программы и разрешает или запрещает запуск этих программ. Задача Контроль запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются.

Вы можете разрешить запуск программ одним из следующих способов:

- задать разрешающие правила для доверенных программ;
- проверять репутацию доверенных программ в KSN при их запуске.

Запрет запуска программы имеет в задаче более высокий приоритет. Например, если запуск программы запрещен одним из правил, программа не будет запущена, независимо от заключения KSN о доверенности программы. При этом если программа признана недоверенной службами KSN, но подпадает под действие разрешающего правила, запуск такой программы будет разрешен.

Все попытки запуска программ фиксируются в журнале выполнения задачи (см. раздел "О журналах выполнения задач" на стр. [250](#)).

Задача Контроль запуска программ может выполняться в одном из двух режимов:

- **Активный** Kaspersky Security для Windows Server с помощью набора правил контролирует запуск программ, которые попадают под действия правил контроля запуска программ. Область применения правил контроля запуска программ указывается в параметрах этой задачи. Если программа



удовлетворяет правилам контроля запуска программ, а параметры задачи не удовлетворяют ни одному из указанных правил, то запуск такой программы будет запрещен.

Запуск программ, которые не подпадают под действие правил, указанных в параметрах задачи Контроль запуска программ, разрешен, независимо от параметров задачи Контроль запуска программ.

**Задачу *Контроль запуска программ* нельзя запустить в активном режиме, если не создано ни одного правила или если для одного защищаемого устройства создано более 65535 правил.**

- **Только статистика** В Kaspersky Security для Windows Server не используются правила контроля запуска программ для запрета или разрешения запуска программ. Выполняется только запись информации обо всех запусках программ, правилах, выполненных при запуске программ, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Активный**. Разрешен запуск всех программ. Этот режим установлен по умолчанию.

Вы можете использовать этот режим для формирования правил контроля запуска программ (см. раздел "Формирование разрешающих правил по событиям задачи Контроль запуска программ" на стр. [472](#)) на основе информации, зафиксированной в журнале выполнения задачи.

Вы можете настроить задачу Контроль запуска программ по одному из следующих сценариев:

- дополнительная настройка и применение правил контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. [425](#));
- базовая настройка правил и использование KSN (см. раздел "Настройка использования KSN" на стр. [464](#)) для Контроля запуска программ.

**Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.**

Kaspersky Security для Windows Server также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ фиксирует запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

## О правилах контроля запуска программ

### Как работают правила контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.  
Правила контроля запуска программ могут разрешить или запретить запуск программы. Соответственно, они называются *разрешающими* или *запрещающими*. Для создания списка разрешающих правил контроля запуска программ можно использовать задачу формирования разрешающих правил или задачу Контроль запуска программ в режиме **Только статистика**. Можно также добавлять разрешающие правила вручную.

- Пользователь и / или группа пользователей.

Правила контроля запуска программ контролируют запуск указанных программ пользователем или группой пользователей.

- Область применения правила.

Правила контроля запуска программ могут применяться к *исполняемым файлам, скриптам и пакетам MSI*.

- Критерий срабатывания правила.

Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих одному из указанных в параметрах правила критериев: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

Если в качестве критерия срабатывания правила выбран **Цифровой сертификат**, созданное правило контролирует запуск всех доверенных программ в операционной системе. Вы можете задать более строгие условия для этого критерия, установив следующие флажки:

- **Использовать заголовок**

Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывание правил запуска программ на основе цифрового сертификата, поскольку отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для определенных разрешающих правил: например, если требуется разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

## Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

## О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программного обеспечения на защищаемых устройствах, например, на защищаемых устройствах, где происходит регулярное автоматическое обновление установленного программного обеспечения. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения можно использовать подсистему Контроль пакетов установки.

*Пакет установки* (далее также "пакет") представляет собой программу, устанавливаемую на защищаемое устройство. В каждом пакете содержится как минимум одна программа, а также могут содержаться отдельные файлы, обновления и отдельные команды, в частности, когда выполняется установка программы или обновления.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. При добавлении пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета

установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Security для Windows Server контролирует только полный цикл распространения программного обеспечения. Программа не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен компонент Контроль пакетов установки или не был установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в параметрах задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

## Кеш распространения программного обеспечения

Kaspersky Security для Windows Server использует динамически формируемый кеш распространения программного обеспечения (далее "кеш распространения") для связи между доверенными пакетами и файлами, созданными во время распространения программного обеспечения. При первом запуске пакета Kaspersky Security для Windows Server обнаруживает все файлы, созданные этим пакетом во время распространения программного обеспечения, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем, по умолчанию, разрешается запуск всех файлов в кеше распространения.

Кеш распространения нельзя просматривать, очищать и изменять вручную через пользовательский интерфейс. Kaspersky Security для Windows Server самостоятельно наполняет его, а также контролирует его актуальность.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и очищать с помощью команд командной строки.

- Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

- Чтобы полностью очистить кеш распространения, выполните команду:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Security для Windows Server обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла программа удаляет запись для этого файла из кеша распространения. При активном режиме работы задачи Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

## Обработка извлеченных файлов

Все извлеченные из доверенного пакета файлы наследуют атрибут доверенности при первом запуске пакета. При снятии флажка после первого запуска все извлеченные из пакета файлы сохраняют атрибут наследования. Чтобы отменить признак наследования для всех извлеченных файлов, необходимо очистить кеш распространения и снять флажок **Разрешить запуск всех файлов, извлеченных из этого пакета установки** перед следующим запуском доверенного пакета установки.

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки, наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными. По умолчанию количество уровней наследования признака доверенности не ограничено.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 442) с помощью флажка **Разрешать исполнение всей цепочки файлов, извлеченных из этого пакета установки**.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и установлен флажок, то все пакеты и программы, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешить запуск всех файлов, извлеченных из этого пакета установки** не установлен, программа присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (только первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

## Работа со списком правил контроля запуска программ

Список доверенных пакетов подсистемы Контроля пакетов установки – это список исключений, который дополняет, но не заменяет основной список правил контроля запуска программ.

Запрещающие правила контроля запуска программ имеют абсолютный приоритет: распаковка доверенного пакета или запуск созданных и измененных им файлов будут заблокированы, если такие пакеты и файлы подпадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

## Использование заключений KSN

Заключения KSN о том, что файл является недоверенным, имеют более высокий приоритет, чем исключения Контроля пакетов установки. Распаковка доверенных пакетов и запуск файлов, созданных или измененных доверенными пакетами, будет заблокирован, если для таких файлов получено заключение KSN о том, что файл является недоверенным.

При распаковке из доверенного пакета, запуск всех вложенных файлов будет разрешен, независимо от использования KSN в задаче Контроль запуска программ. При этом значение флажков **Блокировать**

запуск программ, недоверенных в KSN и Разрешать запуск программ, доверенных в KSN не влияет на флажок Разрешить запуск всех файлов, извлеченных из этого пакета установки.

## Об использовании KSN в задаче Контроль запуска программ

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Если данные KSN о репутации программы используются в задаче Контроль запуска программ, репутация программы по данным KSN считается основным критерием для разрешения или запрета запуска этой программы. Если KSN передает Kaspersky Security для Windows Server данные о том, что программа не является доверенной, то попытка пользователя запустить программу блокируется. Если KSN передает Kaspersky Security для Windows Server данные о том, что программа является доверенной, то разрешается запуск программы пользователем. KSN можно применять совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

### Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом устройстве без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Security для Windows Server вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом запрета по умолчанию. Применение KSN при отсутствии правил позволяет защитить устройство от программ, которые по данным KSN представляют угрозу.

### Применение заключений KSN совместно с правилами контроля запуска программ

При использовании заключений KSN совместно с правилами контроля запуска программ применяются следующие условия:

- Kaspersky Security для Windows Server всегда блокирует запуск программы, если она подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволит расширить список заблокированных программ.
- Kaspersky Security для Windows Server всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для этой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить устройство от программ, которые по данным KSN представляют угрозу, но не были учтены при первоначальной настройке правил.

## О формировании правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых устройств и групп защищаемых устройств в сети организации. Рекомендуется использовать перечисленные сценарии, если в сети организации нет эталонной машины и вы не можете сформировать список разрешающих правил на основе программ, установленным на такой эталонной машине.

Можно запустить задачу Формирование правил контроля запуска программ локально с помощью Консоли программы для создания списка правил на основе программ, запущенных на отдельном защищаемом устройстве.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающее правило для скриптов и пакетов установщика Windows с сертификатом, доверенным в операционной системе.
- Разрешающее правило для исполняемых файлов с сертификатом, доверенным в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи Формирование правил контроля запуска программ.

В рамках этого сценария групповая задача формирует собственный список правил контроля запуска программ для каждого защищаемого устройства в сети и сохраняет эти списки в XML-файл в указанной папке общего доступа. XML-файл, созданный задачей Формирование правил контроля запуска программ, содержит разрешающие правила, указанные при настройке параметров задачи, до ее запуска. Для программ, запуск которых не разрешен в параметрах указанной задачи, не будет создано ни одного правила. Запуск таких программ будет заблокирован по умолчанию. Затем вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ для политики Kaspersky Security Center.

Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Рекомендуется использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

- На основе отчета о событиях в работе задачи Контроль запуска программ в режиме **Только статистика**, сформированного в Kaspersky Security Center.

В рамках этого сценария Kaspersky Security для Windows Server не блокирует запуск программ. Когда задача Контроль запуска программ работает в режиме **Только статистика**, все разрешенные



и запрещенные запуски программ на всех защищаемых устройствах сети регистрируются на закладке **События** в рабочей области узла Сервера администрирования в Kaspersky Security Center. С помощью отчетов в Kaspersky Security Center формируется единый список событий о заблокированных запусках программ.

Вам нужно настроить период выполнения задачи так, чтобы за указанный промежуток времени выполнились все возможные сценарии работы защищаемых устройств и групп защищаемых устройств и хотя бы одна перезагрузка. После завершения выполнения задачи можно импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

Рекомендуется использовать этот сценарий, если в сети организации имеется большое количество защищаемых устройств разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на защищаемом устройстве должна находиться под управлением активной политики Kaspersky Security Center. При этом все события на защищаемом устройстве передаются на Сервер администрирования.

Рекомендуется обновить список правил при изменении состава программ, установленных на управляемых устройствах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется сформировать обновленный список правил, запустив задачу Формирование правил контроля запуска программ или задачу Контроль запуска программ в режиме **Только статистика** на защищаемых устройствах тестовой группы администрирования. Тестовая группа администрирования включает защищаемые устройства, необходимые для тестового запуска новых программ перед их установкой на остальные защищаемые устройства сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа задач, запускаемых на защищаемом устройстве. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуется запускать задачи Формирование правил контроля запуска программ и Контроль запуска программ в режиме **Только статистика** на эталонной машине.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.



## Параметры по умолчанию для задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 72. Параметры по умолчанию для задачи Контроль запуска программ

| Параметр                                                                                          | Значение по умолчанию                                                                                                                                                                                         | Описание                                                                                                       |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Режим работы задачи</b>                                                                        | <b>Только статистика</b> Задача регистрирует события, соответствующие попыткам запуска программ, запрещенным или разрешенным на основе набора правил. Фактическая блокировка запуска программ не выполняется. | Вы можете выбрать режим <b>Активный</b> после того, как будет сформирован окончательный список правил.         |
| <b>Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках</b> | Применяется.                                                                                                                                                                                                  | Можно повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках.              |
| <b>Запретить запуск командных интерпретаторов без команд к исполнению</b>                         | Не применяется.                                                                                                                                                                                               | Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.                                   |
| <b>Управление правилами</b>                                                                       | <b>Заменить правилами политики локальные правила.</b>                                                                                                                                                         | Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на защищаемом устройстве. |

| Параметр                                                                                                       | Значение по умолчанию                                                                                                                          | Описание                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Область применения правил</b>                                                                               | Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов. Кроме того, она контролирует загрузку DLL-модулей.                      | Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.                                                                                                                                       |
| <b>Использование KSN</b>                                                                                       | Данные KSN о репутации программы не используются.                                                                                              | Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.                                                                                                                   |
| <b>Автоматически разрешать распространение для программ и пакетов из списка</b>                                | Не применяется.                                                                                                                                | Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию распространение программ разрешено только с помощью служб установщика Windows. |
| <b>Всегда разрешать распространение программ через установщик Windows</b>                                      | Применяется. Можно изменить, только если включен параметр <b>Автоматически разрешать распространение для программ и пакетов из списка</b> .    | Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются с помощью установщика Windows.                                                                                  |
| <b>Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи</b> | Не применяется. Можно изменить, только если включен параметр <b>Автоматически разрешать распространение для программ и пакетов из списка</b> . | Можно включить или выключить автоматическое распространение программного обеспечения с помощью решения System Center Configuration Manager.                                                                             |
| <b>Запуск задачи</b>                                                                                           | Время первого запуска не задано.                                                                                                               | Задача Контроль запуска программ не запускается автоматически сразу после Kaspersky Security для Windows Server. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.                          |

Table 73. Заданные по умолчанию параметры задачи Формирование правил контроля запуска программ

| Параметр                                 | Значение по умолчанию                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Описание                                                                                                                                                                                                                                               |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Префикс для названий разрешающих правил  | Совпадает с именем защищаемого устройства, на котором установлена программа Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                                                                                          | Вы можете изменить префикс для названий разрешающих правил.                                                                                                                                                                                            |
| Область применения разрешающих правил    | <p>Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов:</p> <ul style="list-style-type: none"> <li>• файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files;</li> <li>• пакеты MSI, расположенные в папке C:\Windows;</li> <li>• скрипты, расположенные в папке C:\Windows.</li> </ul> <p>Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.</p> | Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых будет разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы. |
| Критерии формирования разрешающих правил | Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.                                                                                                                                                                                                                                                                                                                                                                 | <p>Вы можете использовать хеш SHA256 при формировании разрешающих правил.</p> <p>Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.</p>                                      |
| Действия по завершении задачи            | Разрешающие правила добавляются в список правил контроля запуска программ; новые правила объединяются с существующими правилами; дублирующиеся правила удаляются.                                                                                                                                                                                                                                                                                                                           | Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующихся правил или заменять существующие правила новыми разрешающими правилами, а также настраивать параметры экспорта разрешающих правил в файл.         |
| Параметры запуска задачи с правами       | Задача запускается с правами системной учетной записи.                                                                                                                                                                                                                                                                                                                                                                                                                                      | Вы можете разрешить запуск задачи Формирование правил контроля запуска программ с правами системной учетной                                                                                                                                            |

| Параметр                  | Значение по умолчанию            | Описание                                                                                                                                                                                                           |
|---------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           |                                  | записи или с правами указанного пользователя.                                                                                                                                                                      |
| Расписание запуска задачи | Время первого запуска не задано. | Задача Формирование правил контроля запуска программ не запускается автоматически при запуске Kaspersky Security для Windows Server. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |

## Управление контролем запуска программ с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

### В этом разделе

|                                                                              |                     |
|------------------------------------------------------------------------------|---------------------|
| Навигация .....                                                              | <a href="#">436</a> |
| Настройка параметров задачи Контроль запуска программ .....                  | <a href="#">438</a> |
| Настройка Контроля пакетов установки .....                                   | <a href="#">442</a> |
| Настройка задачи Формирование правил контроля запуска программ.....          | <a href="#">444</a> |
| Настройка правил контроля запуска программ в Kaspersky Security Center ..... | <a href="#">446</a> |
| Создание задачи Формирование правил контроля запуска программ .....          | <a href="#">455</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                                                                      |                     |
|------------------------------------------------------------------------------------------------------|---------------------|
| Переход к параметрам политики для задачи Контроль запуска программ .....                             | <a href="#">437</a> |
| Переход к списку правил контроля запуска программ .....                                              | <a href="#">437</a> |
| Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам ..... | <a href="#">438</a> |

## Переход к параметрам политики для задачи Контроль запуска программ

- Чтобы перейти к параметрам задачи **Контроль запуска программ** в политике **Kaspersky Security Center**, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

Откроется окно **Контроль запуска программ**.

Настройте политику в соответствии с вашими требованиями.

## Переход к списку правил контроля запуска программ

- Чтобы перейти к списку правил контроля запуска программ в **Kaspersky Security Center**, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

Откроется окно **Контроль запуска программ**.

7. На закладке **Общие** нажмите на кнопку **Список правил**.

Откроется окно **Правила контроля запуска программ**.

Настройте список правил в соответствии с вашими требованиями.

## Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам

► Чтобы создать задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

Откроется окно **Мастер создания задачи**.

5. Выберите задачу **Формирование правил контроля запуска программ**.
6. Нажмите на кнопку **Далее**.

Откроется окно **Параметры**.

► Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

Откроется окно **Свойства: Формирование правил контроля запуска программ**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля запуска программ.

## Настройка параметров задачи Контроль запуска программ

► Чтобы настроить общие параметры задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Контроль запуска программ** (см. раздел "Переход к параметрам политики для задачи Контроль запуска программ" на стр. [437](#)).
2. На закладке **Общие** в разделе **Режим работы задачи** настройте следующие параметры:
  - В раскрывающемся списке **Режим работы задачи** выберите режим работы задачи.

В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:

- **Активный** Kaspersky Security для Windows Server использует определенные правила контроля запуска всех программ.
- **Только статистика** Kaspersky Security для Windows Server не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы

можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.

По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

- Снимите или установите флажок **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет программу при каждой попытке ее запуска.

По умолчанию флажок установлен.

- Снимите или установите флажок **Запретить запуск командных интерпретаторов при отсутствии команд**.

Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

- Запуск командного интерпретатора разрешен.
- Исполняемая команда разрешена.

Если флажок снят, Kaspersky Security для Windows Server учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Security для Windows Server работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

3. В блоке **Управление правилами** настройте параметры применения правил:
  - a. Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила в задачу Контроль запуска программ.

Kaspersky Security для Windows Server не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

b. Выберите режим применения правил:

- **Заменить локальные правила правилами политики**

Программа применяет список правил, заданных в политике, для централизованного контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.

- **Добавить правила политики к локальным правилам**

Программа применяет список правил, заданный в политике, совместно с локальными списками правил. Вы можете редактировать локальные списки правил с помощью задач автоматического формирования правил контроля запуска программ.

По умолчанию Kaspersky Security для Windows Server применяет два стандартных правила, которые разрешают запуск скриптов, MSI-пакетов и исполняемых файлов, если эти объекты подписаны доверенной цифровой подписью.

4. В блоке **Область применения правил** укажите следующие параметры:

- **Применять правила к исполняемым файлам**

Флажок включает или выключает контроль запуска исполняемых файлов.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**

Флажок включает или выключает контроль загрузки DLL-модулей.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Security для Windows Server не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

Флажок доступен, если установлен флажок **Применять правила к исполняемым файлам**.

По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Применять правила к скриптам и пакетам MSI**

Флажок включает или выключает запуск скриптов и пакетов MSI.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.



Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

По умолчанию флажок установлен.

5. В блоке параметров **Использование KSN** настройте следующие параметры запуска программ:

- **Блокировать запуск программ, недоверенных в KSN**

Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- **Разрешать запуск программ, доверенных в KSN**

Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

Если флажок установлен, Kaspersky Security для Windows Server разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые попадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ

6. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка контроля пакетов установки" на стр. [442](#)).

7. На закладке **Управление задачами** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. [142](#)).

8. В окне **Контроль запуска программ** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## Настройка Контроля пакетов установки

► Чтобы добавить доверенный пакет установки, выполните следующие действия:

1. Откройте окно **Контроль запуска программ** (см. раздел "Переход к параметрам политики для задачи Контроль запуска программ" на стр. [437](#)).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение указанных программ и пакетов установки**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки, разрешенных к запуску, доступен для редактирования.

Если флажок снят, программа не применяет указанные в списке исключения.

По умолчанию флажок снят.

Вы можете установить флажок **Автоматически разрешать распространение указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Применять правила к исполняемым файлам**.

3. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью установщика Windows.

Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

По умолчанию флажок установлен.

Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

Если флажок установлен, Kaspersky Security для Windows Server автоматически

разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

Программа контролирует запуск объектов со следующими расширениями:

- exe;
- msi.

По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

- **Добавить один вручную.**

a. Нажмите на кнопку **Обзор**.

b. Выберите исполняемый файл или пакет установки.

Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

c. Снимите или установите флажок **Разрешить запуск всех файлов, извлеченных из этого пакета установки**.

d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

- **Использовать цифровой сертификат**
- **Использовать хеш SHA256**

- **Добавить несколько по хешу**

Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Security для Windows Server учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Security для Windows Server такой файл должен удовлетворять следующим условиям:

- иметь расширение TXT;
- содержать информацию в виде списка строк, каждая из которых – данные для

- одного доверенного файла;
- содержать список, соответствующий одному из двух форматов:
  - <имя файла>:<хеш SHA256>.
  - <хеш SHA256>\*<имя файла>.

В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Настройка задачи Формирование правил контроля запуска программ

► Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 438).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

3. В разделе **Настройка** можно настроить следующие параметры:

- Укажите префикс для названий правил.
- Выберите способ создания разрешающих правил:
  - **Создавать разрешающие правила на основе запущенных программ**

Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

По умолчанию флажок установлен.

Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

- **Создавать разрешающие правила для программ из папок**

В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

4. В разделе **Параметры** можно указать действия при формировании разрешающих правил контроля запуска программ:

- **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Security для Windows Server разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

- **Хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
- **Путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые

находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Параметры**.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Создавать правила для пользователя или группы пользователей**

Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

По умолчанию выбрана группа **Все**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Security для Windows Server создает по завершении задач.

1. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
2. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
3. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

4. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

## Настройка правил контроля запуска программ в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

## В этом разделе

|                                                                                      |                     |
|--------------------------------------------------------------------------------------|---------------------|
| Добавление правила контроля запуска программ.....                                    | <a href="#">447</a> |
| Включение режима разрешения по умолчанию.....                                        | <a href="#">450</a> |
| Создание разрешающих правил на основе событий Kaspersky Security Center .....        | <a href="#">450</a> |
| Импорт правил из отчета Kaspersky Security Center о заблокированных программах ..... | <a href="#">451</a> |
| Импорт правил контроля запуска программ из XML-файла .....                           | <a href="#">453</a> |
| Проверка запуска программ.....                                                       | <a href="#">455</a> |

## Добавление правила контроля запуска программ

► Чтобы добавить правило контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. [437](#)).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.  
Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
  - a. В поле **Название** введите название правила.
  - b. В раскрывающемся списке **Тип** выберите тип правила:
    - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
    - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
  - c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
    - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
    - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
  - d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
    - i. Нажмите на кнопку **Обзор**.
    - ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
    - iii. Задайте список пользователей и / или групп пользователей.
    - iv. Нажмите на кнопку **ОК**.
  - e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:



- i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.  
Откроется стандартное окно Microsoft Windows **Открыть**.
- ii. Выберите файл.
- iii. Нажмите на кнопку **Открыть**.  
Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.
- f. В блоке параметров **Критерий срабатывания правила** выберите один из следующих вариантов:
  - **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
    - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
    - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
  - **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
  - **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.

Kaspersky Security для Windows Server не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

- g. Если вы хотите добавить исключения из правила, выполните следующие действия:
  - i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.  
Откроется окно **Исключение из правила**.
  - ii. В поле **Название** введите название исключения.
  - iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.
    - **Цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок**  
Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.



Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

- Нажмите на кнопку **ОК**.
- Повторите пункты (i)-(iv) для добавления дополнительных исключений.

1. В окне **Параметры правила** нажмите на кнопку **ОК**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

## Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. [437](#)).
2. Нажмите на кнопку **Добавить** и в открывшемся контекстном меню выберите пункт **Добавить правило**.  
Откроется окно **Параметры правила**.
3. В поле **Название** введите название правила.
4. В раскрывающемся списке **Тип** выберите элемент **Разрешающее правило**.
5. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
  - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
  - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
6. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
7. Введите следующую маску: `? : \`
8. В окне **Параметры правила** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server применяет режим разрешения по умолчанию.

## Создание разрешающих правил на основе событий Kaspersky Security Center

► *Чтобы сформировать разрешающие правила контроля запуска программ для программ из событий Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. [437](#)).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
3. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:
  - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

Откроется окно **Формирование правил контроля запуска программ**.

4. Настройте следующие параметры запроса:

- **Адрес Сервера администрирования**
- **Порт**
- **Пользователь**
- **Пароль**

5. Выберите типы событий, которые должны стать основой для задачи формирования правил:

- **Режим Только статистика: запуск программы запрещен.**
- **Запуск программы запрещен.**

6. Выберите период из раскрывающегося списка **Запрашивать события, созданные в течение периода**.

7. Нажмите на кнопку **Создать правила**.

8. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Список правил в задаче Контроль запуска программ будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

Если список правил контроля запуска программ уже задан в политике, Kaspersky Security для Windows Server добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с повторяющимся хешем не добавляются, поскольку все правила в списке должны быть уникальными.

## Импорт правил из отчета Kaspersky Security Center о заблокированных программах

Вы можете импортировать данные о заблокированных запусках программ из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль запуска программ в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил запуска программ в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль запуска программ, вы можете отслеживать программы, запуск которых был заблокирован.

При импорте из отчета данных о заблокированных программах в свойства политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

- Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Контроль запуска программ** (см. раздел "Переход к параметрам политики для задачи Контроль запуска программ" на стр. 437).
2. В блоке **Режим работы задачи** выберите режим **Только статистика**.
3. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что:
  - Для событий с уровнем важности **Критический** срок хранения событий **Запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).
  - Для событий с уровнем важности **Предупреждение** срок хранения событий **Только статистика: запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

По истечении срока хранения событий информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль запуска программ в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленный срок хранения указанных событий.

4. По завершении задачи выполните экспорт зарегистрированных событий в файл формата TXT:
  - a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.
  - b. Нажмите на кнопку **Создать выборку**, чтобы создать выборку событий по критерию Заблокировано и просмотреть, запуск каких программ будет заблокирован задачей Контроль запуска программ.
  - c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых требуется разрешить.

5. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:
  - a. На закладке **Общие** нажмите на кнопку **Список правил**.  
Откроется окно **Правила контроля запуска программ**.
  - b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.
  - c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку настроенных ранее правил контроля запуска программ:
    - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.
- d. В открывшемся стандартном окне Microsoft Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.
- e. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

## Импорт правил контроля запуска программ из XML-файла

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Формирование правил контроля запуска программ, и применить их в качестве списка разрешающих правил в настраиваемой политике.

По завершении групповой задачи формирования правил контроля запуска программ выполняется экспорт созданных разрешающих правил в XML-файлы в указанную папку общего доступа. Каждый файл со списком правил создается на основе анализа исполняемых файлов и запущенных программ на каждом отдельном защищаемом устройстве в сети организации. Списки содержат разрешающие правила для файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче формирования правил контроля запуска программ.

► *Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** панели результатов настраиваемой группы защищаемых устройств создайте групповую задачу Формирование правил контроля запуска программ или выберите существующую задачу (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. [438](#)).
2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
  - В разделе **Уведомление** настройте параметры сохранения отчета выполнения задачи.

Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

- В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Можно изменить набор папок, содержащих разрешенные для запуска программы: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
- В разделе **Параметры** укажите действия, выполняемые задачей во время работы и после завершения. Укажите критерий формирования правил и имя файла, в который будут экспортированы эти правила.
- В разделе **Расписание** настройте параметры запуска задачи по расписанию.

- В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
- В блоке **Исключения из области действия задачи** задайте группы защищаемых устройств, которые вы хотите исключить из области действия задачи.

Kaspersky Security для Windows Server не будет создавать разрешающие правила по программам, запускаемым на исключенных защищаемых устройствах.

3. На закладке **Задачи** панели результатов настраиваемой группы защищаемых устройств в списке групповых задач выберите созданную задачу **Формирование правил контроля запуска программ** и нажмите на кнопку **Запустить** для запуска задачи.

После завершения задачи, автоматически сформированные списки разрешающих правил будут сохранены в XML-файлы в папке общего доступа.

Перед запуском задачи **Контроль запуска программ в сети** убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу **Формирование правил контроля запуска программ** на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

4. Чтобы добавить сформированные списки разрешающих правил в задачу **Контроль запуска программ**, выполните следующие действия:
  - a. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. [437](#)).
  - b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из XML-файла**.
  - c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:
    - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
    - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
    - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.
  - d. В открывшемся стандартном окне Microsoft Windows выберите XML-файлы, созданные по завершении групповой задачи **Формирование правил контроля запуска программ**.
  - e. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.
5. Если вы хотите применять созданные правила для контроля запуска программ, в политике в свойствах задачи **Контроль запуска программ** выберите режим **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном защищаемом устройстве, будут применены на всех защищаемых устройствах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых устройств программа разрешит запуск только тех программ, для которых созданы разрешающие правила.

## Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу, чтобы определить, какие правила контроля запуска программ срабатывают для выбранной программы.

По умолчанию Kaspersky Security для Windows Server блокирует программы, запуск которых не разрешен хотя бы одним правилом. Чтобы избежать блокировки запуска важных программ, необходимо создать для них разрешающие правила.

Если запуск программы контролируется несколькими правилами разных типов, запрещающие правила имеют больший приоритет: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы проверить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. [437](#)).
2. В открывшемся окне нажмите на кнопку **Показать правила для файла**.  
Откроется стандартное окно Microsoft Windows.
3. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все правила, которые сработают при запуске указанного файла.

## Создание задачи Формирование правил контроля запуска программ

► *Чтобы создать задачу Формирование правил контроля запуска программ и настроить ее параметры, выполните следующие действия:*

1. Откройте окно **Параметры** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. [438](#)).
2. Настройте следующие параметры:
  - Укажите **Префикс для названий правил**.  
Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.  
По умолчанию в качестве префикса указано имя защищаемого устройства, на котором установлена программа Kaspersky Security для Windows Server. Вы можете изменить префикс для названий разрешающих правил.
  - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. [474](#)).
3. Нажмите на кнопку **Далее**.
4. Укажите действия, которые должна выполнять программа Kaspersky Security для Windows Server:
  - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. [475](#));



- по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. [477](#)).
- 5. В окне **Расписание** укажите параметры запуска задачи по расписанию.
- 6. Нажмите на кнопку **Далее**.
- 7. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
- 8. Нажмите на кнопку **Далее**.
- 9. Укажите название задачи.
- 10. Нажмите на кнопку **Далее**.

Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " \* < > & \ : |

Откроется окно **Завершение создания задачи**.

11. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
12. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

► Чтобы настроить существующее правило в *Kaspersky Security Center*,

откройте окно **Свойства: Формирование правил контроля запуска программ** и настройте параметры, как описано выше.

Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

|                                                                 |                     |
|-----------------------------------------------------------------|---------------------|
| Ограничение области действия задачи .....                       | <a href="#">456</a> |
| Действия при автоматическом формировании правил .....           | <a href="#">457</a> |
| Действия по завершении автоматического формирования правил..... | <a href="#">459</a> |

## Ограничение области действия задачи

► Чтобы ограничить область действия задачи *Формирование правил контроля запуска программ*, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. [438](#)).
2. Выберите способ создания разрешающих правил:
  - **Создавать разрешающие правила на основе запущенных программ**  
Флажок включает или выключает формирование правил контроля запуска программ



для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

По умолчанию флажок установлен.

Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

- **Создавать разрешающие правила для программ из папок**

В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

3. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Действия при автоматическом формировании правил

► Чтобы настроить действия Kaspersky Security для Windows Server во время выполнения задачи *Формирование правил контроля запуска программ*, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел **"Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам"** на стр. [438](#)).
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:

- **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Security для Windows Server разрешит запуск программ, которые

запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

- **Хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
- **Путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Параметры**.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Создавать правила для пользователя или группы пользователей**

Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

По умолчанию выбрана группа **Все**.

1. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Действия по завершении автоматического формирования правил

► Чтобы настроить действия Kaspersky Security для Windows Server по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 438).
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:

- **Добавлять разрешающие правила в список правил контроля запуска программ**

Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

Если флажок установлен, Kaspersky Security для Windows Server добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

Если флажок снят, Kaspersky Security для Windows Server не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

- **Принцип добавления**

Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

- **Добавлять к существующим правилам.** Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Заменять существующие правила.** Правила добавляются вместо существующих правил.
- **Объединять с существующими правилами.** Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**

- **Добавлять информацию о компьютере в имя файла**

Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

По умолчанию флажок установлен.

4. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

# Управление контролем запуска программ с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе

|                                                                     |                     |
|---------------------------------------------------------------------|---------------------|
| Навигация .....                                                     | <a href="#">460</a> |
| Настройка параметров задачи Контроль запуска программ .....         | <a href="#">461</a> |
| Настройка правил контроля запуска программ.....                     | <a href="#">468</a> |
| Настройка задачи Формирование правил контроля запуска программ..... | <a href="#">473</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

## В этом разделе

|                                                                                 |                     |
|---------------------------------------------------------------------------------|---------------------|
| Переход к параметрам задачи Контроль запуска программ .....                     | <a href="#">460</a> |
| Переход к окну с правилами контроля запуска программ .....                      | <a href="#">461</a> |
| Переход к параметрам задачи Формирование правил контроля запуска программ ..... | <a href="#">461</a> |

## Переход к параметрам задачи Контроль запуска программ

- *Чтобы перейти к общим параметрам задачи Контроль запуска программ в Консоли программы, выполните следующие действия:*
  1. В дереве Консоли программы разверните узел **Контроль сервера**.
  2. Выберите вложенный узел **Контроль запуска программ**.
  3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.

## Переход к окну с правилами контроля запуска программ

- Чтобы перейти к списку правил контроля запуска программ в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль сервера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

Откроется окно **Правила контроля запуска программ**.

4. Настройте список правил в соответствии с вашими требованиями.

## Переход к параметрам задачи Формирование правил контроля запуска программ

- Чтобы настроить задачу **Формирование правил контроля запуска программ**, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. Настройте задачу в соответствии с вашими требованиями.

## Настройка параметров задачи Контроль запуска программ

- Чтобы настроить общие параметры задачи **Контроль запуска программ**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Контроль запуска программ" на стр. [460](#)).
2. Настройте следующие параметры задачи:
  - На закладке **Общие**:
    - режим работы задачи **Контроль запуска программ** (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. [462](#));
    - область применения правил в задаче (см. раздел "Настройка области применения задачи Контроль запуска программ" на стр. [463](#));
    - использование KSN (см. раздел "Настройка использования KSN" на стр. [464](#)).
  - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. [465](#)) на закладке **Контроль пакетов установки**.
  - Расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)) на закладках **Расписание** и **Дополнительно**.

3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Изменения параметров задачи будут сохранены.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

|                                                                   |                     |
|-------------------------------------------------------------------|---------------------|
| Выбор режима работы задачи Контроль запуска программ.....         | <a href="#">462</a> |
| Настройка области действия задачи Контроль запуска программ ..... | <a href="#">463</a> |
| Настройка использования KSN .....                                 | <a href="#">464</a> |
| Контроль пакетов установки .....                                  | <a href="#">465</a> |

## Выбор режима работы задачи Контроль запуска программ

- Чтобы настроить режим работы задачи **Контроль запуска программ**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. [460](#)).
2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим работы задачи.

В раскрывающемся списке вы можете выбрать режим работы задачи **Контроль запуска программ**:

- **Активный** Kaspersky Security для Windows Server контролирует все запускаемые программы с помощью заданных правил.
- **Только статистика** Kaspersky Security для Windows Server не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о блокировках, зарегистрированной в журнале выполнения задачи.

По умолчанию задача **Контроль запуска программ** запускается в режиме **Только статистика**.

3. Снимите или установите флажок **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет программу при каждой попытке ее запуска.

По умолчанию флажок установлен.

Kaspersky Security для Windows Server заводит новый список событий в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом, контроль запуска программ осуществляется в соответствии с актуальными параметрами безопасности.

4. Снимите или установите флажок **Запретить запуск командных интерпретаторов при отсутствии команд**.

Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

- Запуск командного интерпретатора разрешен.
- Исполняемая команда разрешена.

Если флажок снят, Kaspersky Security для Windows Server учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Security для Windows Server работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

## Настройка области действия задачи Контроль запуска программ

- Чтобы задать область действия задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Контроль запуска программ" на стр. [460](#)).
2. На закладке **Общие** в блоке **Область применения правил** задайте следующие параметры:
  - **Использовать правила для исполняемых файлов**

Флажок включает или выключает контроль запуска исполняемых файлов.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или

запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**

Флажок включает или выключает контроль загрузки DLL-модулей.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Security для Windows Server не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

Флажок доступен, если установлен флажок **Применять правила к исполняемым файлам**.

По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

Флажок включает или выключает запуск скриптов и пакетов MSI.

Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.

Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

По умолчанию флажок установлен.

3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Настройка использования KSN

► Чтобы настроить использование служб KSN в задаче **Контроль запуска программ**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи **Контроль запуска программ**" на стр. [460](#)).
2. На закладке **Общие** в блоке **Использование KSN** укажите параметры использования служб KSN:
  - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.



Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

Если флажок установлен, Kaspersky Security для Windows Server разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые попадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, укажите пользователей и группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

- а. Нажмите на кнопку **Изменить**.

Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

- б. Задайте список пользователей и / или групп пользователей.
- в. Нажмите на кнопку **ОК**.

3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Контроль пакетов установки

► Чтобы добавить доверенный пакет установки, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Контроль запуска программ" на стр. [460](#)).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение указанных программ и пакетов установки**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки,

разрешенных к запуску, доступен для редактирования.

Если флажок снят, программа не применяет указанные в списке исключения.

По умолчанию флажок снят.

Вы можете установить флажок **Автоматически разрешать распространение указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Применять правила к исполняемым файлам**.

3. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью установщика Windows.

Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

По умолчанию флажок установлен.

Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

Если флажок установлен, Kaspersky Security для Windows Server автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

Программа контролирует запуск объектов со следующими расширениями:

- exe;
- msf.

По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

- **Добавить один вручную.**

- a. Нажмите на кнопку **Обзор**.

- b. Выберите исполняемый файл или пакет установки.

Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

- c. Снимите или установите флажок **Разрешить запуск всех файлов, извлеченных из этого пакета установки**.

- d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

- **Использовать цифровой сертификат**
    - **Использовать хеш SHA256**

- **Добавить несколько по хешу**

Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Security для Windows Server учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Security для Windows Server такой файл должен удовлетворять следующим условиям:

- иметь расширение TXT;
- содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
- содержать список, соответствующий одному из двух форматов:
  - <имя файла>:<хеш SHA256>.
  - <хеш SHA256>\*<имя файла>.

В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Настройка правил контроля запуска программ

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

### В этом разделе

|                                                                                    |                     |
|------------------------------------------------------------------------------------|---------------------|
| Добавление правила контроля запуска программ.....                                  | <a href="#">468</a> |
| Включение режима разрешения по умолчанию.....                                      | <a href="#">471</a> |
| Формирование разрешающих правил по событиям задачи Контроль запуска программ ..... | <a href="#">472</a> |
| Экспорт правил контроля запуска программ.....                                      | <a href="#">472</a> |
| Импорт правил контроля запуска программ из XML-файла .....                         | <a href="#">473</a> |
| Удаление правил контроля запуска программ.....                                     | <a href="#">473</a> |

## Добавление правила контроля запуска программ

► Чтобы добавить правило контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.  
Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
  - a. В поле **Название** введите название правила.
  - b. В раскрывающемся списке **Тип** выберите тип правила:
    - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
    - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
  - c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
    - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.

- **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
- d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
- i. Нажмите на кнопку **Обзор**.
  - ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
  - iii. Задайте список пользователей и / или групп пользователей.
  - iv. Нажмите на кнопку **ОК**.
- e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:
- i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.  
Откроется стандартное окно Microsoft Windows **Открыть**.
  - ii. Выберите файл.
  - iii. Нажмите на кнопку **Открыть**.  
Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.
- f. В блоке параметров **Критерий срабатывания правила** выберите один из следующих вариантов:
- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
    - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
    - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
  - **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
  - **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.
- Kaspersky Security для Windows Server не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.
- g. Если вы хотите добавить исключения из правила, выполните следующие действия:
- i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.  
Откроется окно **Исключение из правила**.
  - ii. В поле **Название** введите название исключения.

- iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок**

Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила

указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

- i. Нажмите на кнопку **ОК**.
- ii. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

1. В окне **Параметры правила** нажмите на кнопку **ОК**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

## Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.  
Откроется окно **Параметры правила**.
4. В поле **Название** введите название правила.
5. В раскрывающемся списке **Тип** выберите элемент **Разрешающее правило**.
6. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
  - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
  - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
7. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
8. Введите следующую маску: `? : \`
9. В окне **Параметры правила** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server применяет режим разрешения по умолчанию.



## Формирование разрешающих правил по событиям задачи Контроль запуска программ

► Чтобы создать конфигурационный файл с разрешающими правилами, сформированный по событиям задачи Контроль запуска программ, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. [462](#)), чтобы зафиксировать в журнале выполнения задачи информацию обо всех запусках программ на защищаемом устройстве.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Security для Windows Server создаст конфигурационный файл в формате XML со списком правил, сформированных на основе событий задачи Контроль запуска программ, отработавшей в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. [473](#)) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть и обработать вручную список правил, чтобы убедиться, что запуск важных файлов (например, файлов операционной системы) разрешен заданными правилами.

Все события задачи фиксируются в журнале выполнения задачи, независимо от режима работы задачи. Вы можете создать конфигурационный файл со списком правил на основе журнала, сформированного во время выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, поскольку финальный список правил должен быть сформирован перед запуском задачи в режиме **Активный**, чтобы правила работали эффективно.

## Экспорт правил контроля запуска программ

► Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Экспортировать в файл**.  
Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, при экспорте правил его содержимое будет перезаписано.
4. Нажмите на кнопку **Сохранить**.

Параметры правил будут экспортированы в указанный файл.



## Импорт правил контроля запуска программ из XML-файла

► Чтобы импортировать правила контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:
  - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
  - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

Откроется стандартное окно Microsoft Windows **Открыть**.

5. В окне **Открыть** выберите XML-файл, содержащий правила контроля запуска программ.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

## Удаление правил контроля запуска программ

► Чтобы удалить правила контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. В списке выберите правила, которые требуется удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

## Настройка задачи Формирование правил контроля запуска программ

► Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. [461](#)) для задачи **Формирование правил контроля запуска программ**.
2. Настройте следующие параметры:

- На закладке **Общие**:
  - Укажите **Префикс для названий правил**.  
 Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.  
 По умолчанию в качестве префикса указано имя защищаемого устройства, на котором установлена программа Kaspersky Security для Windows Server. Вы можете изменить префикс для названий разрешающих правил.
  - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. [474](#)).
- На закладке **Действия** укажите действия, которые должна выполнять программа Kaspersky Security для Windows Server:
  - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. [475](#));
  - по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. [477](#)).
- На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)).
- На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)).

3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после их изменения.

## В этом разделе

|                                                                 |                     |
|-----------------------------------------------------------------|---------------------|
| Ограничение области действия задачи .....                       | <a href="#">474</a> |
| Действия при автоматическом формировании правил .....           | <a href="#">475</a> |
| Действия по завершении автоматического формирования правил..... | <a href="#">477</a> |

## Ограничение области действия задачи

► Чтобы ограничить область действия задачи *Формирование правил контроля запуска программ*, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. [461](#)) для задачи **Формирование правил контроля запуска программ**.
2. Выберите способ создания разрешающих правил:
  - **Создавать разрешающие правила на основе запущенных программ**  
 Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого

вы хотите сформировать разрешающие правила.

Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

По умолчанию флажок установлен.

Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

- **Создавать разрешающие правила для программ из папок**

В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Действия при автоматическом формировании правил

► Чтобы настроить действия Kaspersky Security для Windows Server во время выполнения задачи **Формирование правил контроля запуска программ**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. [461](#)) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:

- **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Security для Windows Server разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

- **Хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
- **Путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Параметры**.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Создавать правила для пользователя или группы пользователей**

Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

По умолчанию выбрана группа **Все**.

1. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Действия по завершении автоматического формирования правил

- Чтобы настроить действия Kaspersky Security для Windows Server по завершении выполнения задачи **Формирование правил контроля запуска программ**, выполните следующие действия:

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. [461](#)) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:

- **Добавлять разрешающие правила в список правил контроля запуска программ**

Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла **Контроль запуска программ**.

Если флажок установлен, Kaspersky Security для Windows Server добавляет правила, сформированные в ходе выполнения задачи **Формирование правил контроля запуска программ**, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

Если флажок снят, Kaspersky Security для Windows Server не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

- **Принцип добавления**

Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

- **Добавлять к существующим правилам.** Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Заменять существующие правила.** Правила добавляются вместо существующих правил.
- **Объединять с существующими правилами.** Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**
- **Добавлять информацию о компьютере в имя файла**

Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

По умолчанию флажок установлен.

4. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

## Управление контролем запуска программ с помощью веб-плагина

Table 74.

- Чтобы настроить задачи контроля запуска программ с помощью веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на серверах**.
5. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.
6. Настройте параметры, приведены в следующей таблице.

Table 75. Параметры задачи Контроль запуска программ

| Параметр            | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Режим работы задачи | <p>В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:</p> <ul style="list-style-type: none"> <li>• <b>Активный</b> Kaspersky Security для Windows Server использует определенные правила контроля запуска всех программ.</li> <li>• <b>Только статистика</b> Kaspersky Security для Windows Server не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.</li> </ul> <p>По умолчанию задача Контроль запуска программ запускается в режиме <b>Только статистика</b>.</p> |

| Параметр                                                                                          | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Повторять действие, выполненное с файлом при первом запуске, при всех последующих запусках</b> | <p>Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.</p> <p>Если флажок снят, Kaspersky Security для Windows Server проверяет программу при каждой попытке ее запуска.</p> <p>По умолчанию флажок установлен.</p> |

| Параметр                                                                  | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Запретить запуск командных интерпретаторов без команд к исполнению</b> | <p>Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:</p> <ul style="list-style-type: none"> <li>• Запуск командного интерпретатора разрешен.</li> <li>• Исполняемая команда разрешена.</li> </ul> <p>Если флажок снят, Kaspersky Security для Windows Server учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.</p> <p>Kaspersky Security для Windows Server работает со следующими командными интерпретаторами:</p> <ul style="list-style-type: none"> <li>• cmd.exe;</li> <li>• powershell.exe;</li> <li>• python.exe;</li> <li>• perl.exe.</li> </ul> <p>По умолчанию флажок снят.</p> |
| <b>Использовать правила для исполняемых файлов</b>                        | <p>Флажок включает или выключает контроль запуска исполняемых файлов.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения <b>Исполняемые файлы</b>.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.</p> <p>По умолчанию флажок установлен.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



| Параметр                                        | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Контролировать загрузку DLL-модулей             | <p>Флажок включает или выключает контроль загрузки DLL-модулей.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения <b>Исполняемые файлы</b>.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.</p> <p>Флажок доступен, если установлен флажок <b>Применять правила к исполняемым файлам</b>.</p> <p>По умолчанию флажок снят.</p> |
| Использовать правила для скриптов и пакетов MSI | <p>Флажок включает или выключает запуск скриптов и пакетов MSI.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.</p> <p>По умолчанию флажок установлен.</p>                                                                   |

| Параметр                                               | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Блокировать запуск программ, недоверенных в KSN</b> | <p>Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.</p> <p>По умолчанию флажок снят.</p>                                                                |
| <b>Разрешать запуск программ, доверенных в KSN</b>     | <p>Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.</p> <p>Если флажок установлен, Kaspersky Security для Windows Server разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.</p> <p>Если флажок снят, Kaspersky Security для Windows Server не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.</p> <p>По умолчанию флажок снят.</p> |
| <b>Правила</b>                                         | <p>Настройте разрешающие и запрещающие правила (см. раздел "Настройка правил контроля запуска программ в Kaspersky Security Center" на стр. <a href="#">446</a>) для задачи контроля запуска программ.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Параметр                   | Описание                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Контроль пакетов установки | Можно добавлять доверенные пакеты установки (см. раздел "Настройка Контроля пакетов установки" на стр. <a href="#">442</a> ). |
| Управление задачами        | Вы можете настроить расписание запуска задачи.                                                                                |

# Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Мониторинг файловых операций.

## В этом разделе

|                                                                              |                     |
|------------------------------------------------------------------------------|---------------------|
| О задаче Мониторинг файловых операций.....                                   | <a href="#">484</a> |
| О правилах мониторинга файловых операций .....                               | <a href="#">485</a> |
| Параметры по умолчанию для задачи Мониторинг файловых операций .....         | <a href="#">487</a> |
| Управление мониторингом файловых операций с помощью Плагина управления ..... | <a href="#">489</a> |
| Управление мониторингом файловых операций с помощью Консоли программы .....  | <a href="#">493</a> |
| Управление мониторингом файловых операций с помощью Веб-плагина .....        | <a href="#">496</a> |

## О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

**Обрыв мониторинга** – это период, когда область мониторинга временно выпадает из поля действия задачи, например, из-за приостановки выполнения задачи или из-за физического отсутствия внешнего устройства на защищаемом устройстве. Kaspersky Security для Windows Server сообщит об обнаружении файловых операций в области мониторинга, как только внешнее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

### Требования к среде

Для запуска задачи Мониторинг файловых операций должны выполняться следующие условия:

- На защищаемом устройстве установлено внешнее устройство, поддерживающее файловую систему ReFS или NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN-журнала компонент получает данные о файловых операциях.

Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинг файловых операций, необходимо перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

## Исключения для области мониторинга

Вы можете создать исключения из области мониторинга (см. раздел "Настройка правил мониторинга" на стр. 490). Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

## О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания правила и регулировать уровень важности событий для обнаруженных файловых операций, регистрируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- доверенные пользователи;
- маркеры файловых операций.

### Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

*Недоверенный пользователь* – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Security для Windows Server обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует Критическое событие в журнале выполнения задачи.

*Доверенный пользователь* – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Security для Windows Server обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует Информационное событие в журнале выполнения задачи.

Kaspersky Security для Windows Server не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

*Неизвестный пользователь* – данный статус присваивается пользователю в случае, когда Kaspersky Security для Windows Server не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Security для Windows Server обнаруживает файловую операцию, выполненную неизвестным пользователем, задача Мониторинг файловых операций фиксирует событие *Предупреждение* в журнале выполнения задачи.

## Маркеры файловых операций

В ходе выполнения задачи Мониторинг файловых операций Kaspersky Security для Windows Server определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа регистрирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Security для Windows Server учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см. таблицу ниже).

Table 76. Маркеры файловых операций

| ID файловой операции | Маркер файловой операции                                           | Поддерживаемые файловые системы |
|----------------------|--------------------------------------------------------------------|---------------------------------|
| BASIC_INFO_CHANGE    | изменены атрибуты или метки времени файла или папки                | NTFS, ReFS                      |
| COMPRESSION_CHANGE   | изменено сжатие файла или папки                                    | NTFS, ReFS                      |
| DATA_EXTEND          | размер файла или папки увеличен                                    | NTFS, ReFS                      |
| DATA_OVERWRITE       | перезаписаны данные в файле или папке                              | NTFS, ReFS                      |
| DATA_TRUNCATION      | файл или папка усечены                                             | NTFS, ReFS                      |
| EA_CHANGE            | изменены расширенные атрибуты файла или папки                      | только NTFS                     |
| ENCRYPTION_CHANGE    | изменен статус шифрования файла или папки                          | NTFS, ReFS                      |
| FILE_CREATE          | файл или папка созданы впервые                                     | NTFS, ReFS                      |
| FILE_DELETE          | Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL | NTFS, ReFS                      |
| HARD_LINK_CHANGE     | жесткая связь создана или удалена для файла или папки              | только NTFS                     |
| INDEXABLE_CHANGE     | изменен статус индексирования файла или папки                      | NTFS, ReFS                      |

| ID файловой операции  | Маркер файловой операции                                                             | Поддерживаемые файловые системы |
|-----------------------|--------------------------------------------------------------------------------------|---------------------------------|
| INTEGRITY_CHANGE      | изменен атрибут целостности для именованного файлового потока                        | только ReFS                     |
| NAMED_DATA_EXTEND     | размер именованного файлового потока увеличен                                        | NTFS, ReFS                      |
| NAMED_DATA_OVERWRITE  | именованный файловый поток перезаписан                                               | NTFS, ReFS                      |
| NAMED_DATA_TRUNCATION | именованный файловый поток усечен                                                    | NTFS, ReFS                      |
| OBJECT_ID_CHANGE      | изменен идентификатор файла или папки                                                | NTFS, ReFS                      |
| RENAME_NEW_NAME       | присвоено новое имя для файла или папки                                              | NTFS, ReFS                      |
| REPARSE_POINT_CHANGE  | создана новая или изменена существующая точка повторного анализа для файла или папки | NTFS, ReFS                      |
| SECURITY_CHANGE       | изменены права доступа к файлу или папке                                             | NTFS, ReFS                      |
| STREAM_CHANGE         | создан новый или изменен существующий именованный файловый поток                     | NTFS, ReFS                      |
| TRANSACTIONED_CHANGE  | именованный файловый поток изменен транзакцией TxF                                   | только ReFS                     |

## Параметры по умолчанию для задачи Мониторинг файловых операций

По умолчанию в задаче Мониторинг файловых операций используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 77. Параметры по умолчанию для задачи Мониторинг файловых операций

| Параметр                                                                        | Значение по умолчанию                               | Описание                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Область мониторинга                                                             | Не задано                                           | Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.                                                                                                                   |
| Список <b>Доверенные пользователи</b>                                           | Не задано                                           | Вы можете задать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.                                                                                                                                            |
| <b>Фиксировать информацию о файловых операциях за период обрыва мониторинга</b> | Применяется                                         | Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.                                                                                                                                             |
| <b>Блокировать попытки компрометации USN-журнала</b>                            | Применяется                                         | Вы можете включать и выключать защиту USN-журнала.                                                                                                                                                                                                                                    |
| <b>Исключить следующие папки из контроля</b>                                    | Не применяется                                      | Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Security для Windows Server будет пропускать области мониторинга, заданные в качестве исключений. |
| <b>Расчет контрольной суммы</b>                                                 | Не применяется                                      | Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.                                                                                                                                                                                               |
| <b>Маркеры файловых операций</b>                                                | Учитываются все доступные маркеры файловых операций | Вы можете задать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Security для Windows Server формирует событие аудита.                                                    |
| Расписание запуска задачи                                                       | Время первого запуска не задано.                    | Вы можете настроить расписание запуска задачи.                                                                                                                                                                                                                                        |



## Управление мониторингом файловых операций с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Плагина управления.

### В этом разделе

|                                                               |                     |
|---------------------------------------------------------------|---------------------|
| Настройка параметров задачи Мониторинг файловых операций..... | <a href="#">489</a> |
| Настройка правил мониторинга.....                             | <a href="#">490</a> |

## Настройка параметров задачи Мониторинг файловых операций

Чтобы настроить общие параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.  
Откроется окно **Мониторинг файловых операций**.
5. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте следующие параметры:
  - a. Снимите или установите флажок **Фиксировать информацию о файловых операциях за период обрыва мониторинга**.

Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

Если флажок установлен, Kaspersky Security для Windows Server будет

фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

По умолчанию флажок установлен.

- b. Снимите или установите флажок **Блокировать попытки компрометации USN-журнала**.
- c. Добавьте области мониторинга (см. раздел "Настройка правил мониторинга" на стр. [490](#)), которые будут контролировать задача.
6. На закладке **Управление задачами** настройте параметры запуска задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. [141](#)).
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

## Настройка правил мониторинга

► Чтобы добавить область мониторинга, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.  
Откроется окно **Мониторинг файловых операций**.
5. В разделе **Область мониторинга** нажмите на кнопку **Добавить**.  
Откроется окно **Правила мониторинга файловых операций**.
6. Добавьте область мониторинга одним из следующих способов:
  - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
    - a. Нажмите на кнопку **Обзор**.  
Откроется стандартное окно Microsoft Windows **Обзор папок**.

- б. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите на кнопку **ОК**.
- Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
  - `<*.ext>` - все файлы с расширением `<ext>`, независимо от их расположения;
  - `<*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>`, независимо от их расположения;
  - `<\dir\*>` - все файлы в папке `<\dir>`;
  - `<\dir\*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>` в папке `<\dir>` и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: `<буква тома>:\<маска>`. Если том не указан, Kaspersky Security для Windows Server не добавит указанную область мониторинга.

7. На закладке **Доверенные пользователи** нажмите на кнопку **Добавить**.  
Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
8. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга, и нажмите на кнопку **ОК**.

По умолчанию Kaspersky Security для Windows Server считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 485), и формирует для них события с уровнем важности **Критический**.

9. Выберите закладку **Маркеры файловых операций**.
10. Если требуется, выберите несколько маркеров, выполнив следующие действия:
  - а. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
  - б. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 485) установите флажки напротив операций, которые вы хотите контролировать.

По умолчанию Kaspersky Security для Windows Server обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

11. Если вы хотите, чтобы программа Kaspersky Security для Windows Server рассчитывала контрольную сумму файла после изменения, выполните следующие действия:
  - а. Установите флажок **По возможности рассчитывать контрольную сумму файла**.  
**Контрольная сумма отображается в отчете о выполнении задачи.**

Если флажок установлен, Kaspersky Security для Windows Server рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаружена сразу по нескольким маркерам,

рассчитывается только окончательная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Security для Windows Server не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

- **Хеш MD5**
- **Хеш SHA256**

12. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. [485](#)) установите флажки напротив операций, которые вы хотите контролировать.

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

a. Выберите закладку **Исключения**.

b. Установите флажок **Исключить следующие папки из контроля**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Security для Windows Server пропускает области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Security для Windows Server фиксирует события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

c. Нажмите на кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите на кнопку **ОК**.

Указанная папка добавится в список исключенных областей.

14. В окне **Правила мониторинга файловых операций** нажмите на кнопку **ОК**.

Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

## Управление мониторингом файловых операций с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Консоли программы.

### В этом разделе

|                                                               |                     |
|---------------------------------------------------------------|---------------------|
| Настройка параметров задачи Мониторинг файловых операций..... | <a href="#">493</a> |
| Настройка правил мониторинга.....                             | <a href="#">494</a> |

## Настройка параметров задачи Мониторинг файловых операций

► Чтобы настроить общие параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** настройте следующие параметры:
  - a. Снимите или установите флажок **Фиксировать информацию о файловых операциях за период обрыва мониторинга**.

Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

Если флажок установлен, Kaspersky Security для Windows Server будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

По умолчанию флажок установлен.
  - b. Снимите или установите флажок **Блокировать попытки компрометации USN-журнала**.
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. [141](#)).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

## Настройка правил мониторинга

► Чтобы добавить область мониторинга, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга файловых операций**.

Откроется окно **Правила мониторинга файловых операций**.

4. Добавьте область мониторинга одним из следующих способов:
  - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
    - a. В левой части окна нажмите на кнопку **Обзор**.  
Откроется стандартное окно Microsoft Windows **Обзор папок**.
    - b. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите на кнопку **ОК**.
    - c. Нажмите кнопку **Добавить**, чтобы программа Kaspersky Security для Windows Server начала контролировать файловые операции в указанной области мониторинга.
  - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
    - `<*.ext>` - все файлы с расширением `<ext>`, независимо от их расположения;
    - `<*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>`, независимо от их расположения;
    - `<\dir\*>` - все файлы в папке `<\dir>`;
    - `<\dir\*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>` в папке `<\dir>` и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: `<буква тома>:\<маска>`. Если том не указан, Kaspersky Security для Windows Server не добавит указанную область мониторинга.

В правой части окна на закладке **Описание правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.

5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.
6. Выберите закладку **Доверенные пользователи**.
7. Нажмите на кнопку **Добавить**.

Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

8. Выберите пользователей или группы пользователей, которые Kaspersky Security для Windows Server будет считать доверенными для выбранной области мониторинга.
9. Нажмите на кнопку **ОК**.

По умолчанию Kaspersky Security для Windows Server считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 485), и формирует для них события с уровнем важности Критический.

10. Выберите закладку **Маркеры файловых операций**.
11. Если требуется, выберите несколько маркеров, выполнив следующие действия:
  - a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
  - b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 485) установите флажки напротив операций, которые вы хотите контролировать.

По умолчанию Kaspersky Security для Windows Server обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Security для Windows Server рассчитывала контрольную сумму файла после изменения, выполните следующие действия:
  - a. В разделе **Контрольная сумма** выберите **Рассчитывать контрольную сумму измененного файла, если это возможно**. Контрольная сумма отображается в журнале выполнения задачи.

Если флажок установлен, Kaspersky Security для Windows Server рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Security для Windows Server не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

    - если файл стал недоступен (например, в результате изменения прав доступа к файлу);
    - если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.
  - b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих вариантов:
    - **Хеш MD5**
    - **Хеш SHA256**
13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
  - a. Выберите закладку **Задать исключения**.
  - b. Установите флажок **Учитывать исключенные области мониторинга**.

Флажок выключает применение исключений для папок, в которых не требуется

мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Security для Windows Server пропускает области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Security для Windows Server фиксирует события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

- c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Обзор папок**.

- d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.
- e. Нажмите на кнопку **ОК**.
- f. Нажмите на кнопку **Добавить**.

Указанная папка добавится в список исключенных областей.

Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

- 14. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры правил.

## Управление мониторингом файловых операций с помощью Веб-плагина

В этом разделе описана настройка задачи Мониторинг файловых операций с помощью Веб-плагина.

### В этом разделе

|                                                    |                     |
|----------------------------------------------------|---------------------|
| Настройка задачи Мониторинг файловых операций..... | <a href="#">496</a> |
| Настройка правил мониторинга.....                  | <a href="#">497</a> |

## Настройка задачи Мониторинг файловых операций

- Чтобы настроить задачу Мониторинг файловых операций с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Настройка** в подразделе **Мониторинг файловых операций**.



6. В открывшемся окне **Мониторинг файловых операций** на закладке **Параметры мониторинга файловых операций** настройте следующие параметры:

- а. Снимите или установите флажок **Фиксировать информацию о файловых операциях за период обрыва мониторинга**.

Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

Если флажок установлен, Kaspersky Security для Windows Server будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

По умолчанию флажок установлен.

- б. Снимите или установите флажок **Блокировать попытки компрометации USN-журнала**.
7. На закладке **Управление задачами** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. [141](#)).
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

## Настройка правил мониторинга

► Чтобы добавить область мониторинга, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Настройка** в подразделе **Мониторинг файловых операций**.
6. В открывшемся окне **Мониторинг файловых операций** перейдите на закладку **Параметры мониторинга файловых операций**.
7. В разделе **USN-журнал** нажмите на кнопку **Добавить**.  
Откроется окно **Правила мониторинга файловых операций**.
8. В разделе **Контроль файловых операций для области** укажите путь с помощью поддерживаемой маски:
  - `<*.ext>` - все файлы с расширением `<ext>`, независимо от их расположения;
  - `<*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>`, независимо от их расположения;
  - `<\dir\*>` - все файлы в папке `<\dir>`;
  - `<\dir*\name.ext>` - все файлы с именем `<name>` и расширением `<ext>` в папке `<\dir>` и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Security для Windows Server не добавит указанную область мониторинга.

9. На закладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

В поле **Имя пользователя** укажите пользователя.

По умолчанию Kaspersky Security для Windows Server считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 485), и формирует для них события с уровнем важности Критический.

10. Выберите закладку **Маркеры файловых операций**.

11. Если требуется, выберите несколько маркеров, выполнив следующие действия:

- Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
- В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 485) установите флажки напротив операций, которые вы хотите контролировать.

По умолчанию Kaspersky Security для Windows Server обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Security для Windows Server рассчитывала контрольную сумму файла после изменения, выполните следующие действия:

- Установите флажок **По возможности рассчитывать контрольную сумму файла**.  
**Контрольная сумма отображается в отчете о выполнении задачи.**

Если флажок установлен, Kaspersky Security для Windows Server рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Security для Windows Server не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

- В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:
  - Хеш MD5**

- **Хеш SHA256**

13. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. [485](#)) установите флажки напротив операций, которые вы хотите контролировать.
14. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
  - a. Выберите закладку **Исключения**.
  - b. Установите флажок **Исключить следующие папки из контроля**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Security для Windows Server пропускает области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Security для Windows Server фиксирует события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.
  - c. Нажмите на кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.
  - d. На открывшейся справа панели выберите папку, которую вы хотите исключить из области мониторинга.
  - e. Нажмите на кнопку **ОК**.

Указанная папка добавится в список исключенных областей.
15. В окне **Правила мониторинга файловых операций** нажмите на кнопку **ОК**.

Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

# Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

## В этом разделе

|                                                                          |                     |
|--------------------------------------------------------------------------|---------------------|
| О задаче Анализ журналов .....                                           | <a href="#">500</a> |
| Параметры по умолчанию для задачи Анализ журналов .....                  | <a href="#">501</a> |
| Управление правилами анализа журналов с помощью Плагина управления ..... | <a href="#">502</a> |
| Управление правилами анализа журналов с помощью Консоли программы .....  | <a href="#">506</a> |
| Управление правилами анализа журналов с помощью Веб-плагина .....        | <a href="#">508</a> |

## О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Security для Windows Server контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках кибератак.

Kaspersky Security для Windows Server анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами, заданными пользователем, или с параметрами эвристического анализатора, который применяется задачей для анализа журналов.

### Стандартные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью стандартных правил, осуществляющих анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом устройстве, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь стандартных правил. Вы можете включать и выключать любые правила. Нельзя удалять существующие правила и создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Security для Windows Server не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

## Пользовательские правила задачи Анализ журналов

С помощью параметров правил вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил анализа журналов содержит четыре правила. Вы можете включать и выключать эти правила, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

Правило срабатывает при создании новой записи в журнале событий Windows, если в свойствах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

Для каждого правила вы можете задать журнал в журнале событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом журнале. Вы можете выбрать один из стандартных журналов (Программа, Безопасность или Система) или указать пользовательский журнал, введя его имя в поле выбора источника.

Программа не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows.

При срабатывании правила Kaspersky Security для Windows Server фиксирует событие с уровнем важности *Критический* в журнале выполнения задачи Анализ журналов.

По умолчанию в задаче Анализ журналов применяются пользовательские правила.

Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробную информацию можно найти в статье Microsoft <https://technet.microsoft.com/ru-ru/library/cc952128.aspx>.

## Параметры по умолчанию для задачи Анализ журналов

По умолчанию в задаче Анализ журналов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 78. Параметры по умолчанию для задачи Анализ журналов

| Параметр                                                | Значение по умолчанию                            | Описание                                                                                                                                                                                        |
|---------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Применять пользовательские правила для анализа журналов | Применяется.                                     | Пользовательские правила можно включать, отключать, добавлять или изменять.                                                                                                                     |
| Использовать стандартные правила для анализа журналов   | Применяется.                                     | Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве.                                                                |
| Обработка перебора пароля                               | 10 неудачных попыток входа в течение 300 секунд. | Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.                                     |
| Обработка сетевого входа                                | 00:00:00                                         | Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Security для Windows Server расценивает данное действие как аномальную активность. |
| Исключения                                              | Не применяется.                                  | Можно указать пользователей и IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.                                                                          |
| Расписание запуска задачи                               | Время первого запуска не задано.                 | Вы можете настроить расписание запуска задачи.                                                                                                                                                  |

## Управление правилами анализа журналов с помощью Плагина управления

В этом разделе описано добавление и настройка правил анализа журналов с помощью Плагина управления.

### В этом разделе

|                                                                             |                     |
|-----------------------------------------------------------------------------|---------------------|
| Управление стандартными правилами задачи с помощью Плагина управления ..... | <a href="#">503</a> |
| Добавление правил анализа журналов с помощью Плагина управления .....       | <a href="#">504</a> |

## Управление стандартными правилами задачи с помощью Плагина управления

► Чтобы настроить параметры стандартных правил для задачи Анализ журналов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [124](#)).
  - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Анализ журналов** нажмите на кнопку **Настройка**. Откроется окно **Анализ журналов**.
5. Выберите закладку **Стандартные правила**.
6. Снимите или установите флажок **Применять стандартные правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Security для Windows Server применяет эвристический анализатор для обнаружения аномальной активности на защищаемом устройстве.

Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Security для Windows Server применяет стандартные или пользовательские правила для обнаружения аномальной активности.

По умолчанию флажок установлен.

Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.

7. Из списка стандартных правил выберите правила, которые вы хотите применить:
  - Обнаружена возможная попытка взлома пароля с помощью подбора.
  - Обнаружены признаки компрометации журналов Windows.
  - Обнаружена подозрительная активность со стороны новой установленной службы.
  - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
  - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).

- Обнаружены подозрительные изменения привилегированной группы Администраторы.
  - Обнаружена подозрительная активность во время сетевого сеанса входа.
8. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.  
Откроется окно **Анализ журналов**.
  9. В разделе **Обработка перебора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
  10. В разделе **Обработка сетевого входа** укажите начало и конец временного интервала.  
Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Security для Windows Server как аномальная активность.
  11. Выберите закладку **Исключения**.
  12. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    - a. Нажмите на кнопку **Обзор**.
    - b. Выберите пользователя.
    - c. Нажмите на кнопку **ОК**.Указанный пользователь будет добавлен в список доверенных.
  13. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    - a. Введите IP-адрес.
    - b. Нажмите на кнопку **Добавить**.
  14. Указанный IP-адрес будет добавлен в список доверенных.
  15. На закладке **Управление задачами** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [142](#)).
  16. В окне **Анализ журналов** нажмите на кнопку **ОК**.  
Параметры задачи Анализ журналов будут сохранены.

## Добавление правил анализа журналов с помощью Плагина управления

- Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. [124](#)).



- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [129](#)).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Анализ журналов** нажмите на кнопку **Настройка**.  
Откроется окно **Анализ журналов**.
5. На закладке **Пользовательские правила** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Security для Windows Server применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.

Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Security для Windows Server применяет параметры правил по умолчанию.

По умолчанию флажок установлен. Активно только правило обнаружения всплывающих окон программ.

Вы можете контролировать применение стандартных правил для анализа журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.  
Откроется окно **Пользовательское правило анализа журналов**.

7. В разделе **Общие** введите следующие данные нового правила:

- **Имя правила**
- **Источник**

Выберите журнал, события которого будут использоваться для анализа. Доступны следующие журналы событий Windows: Программа, Безопасность, Система.

Вы можете добавить новый пользовательский журнал, указав название журнала в поле **Источник**.

8. В разделе **Идентификаторы событий-триггеров** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
  - a. Укажите идентификатор.
  - b. Нажмите на кнопку **Добавить**.

Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

9. Нажмите на кнопку **ОК**.

Правило анализа журналов добавится в список правил.

## Управление правилами анализа журналов с помощью Консоли программы

В этом разделе описано добавление и настройка правил анализа журналов с помощью Консоли программы.

### В этом разделе

|                                                                            |                     |
|----------------------------------------------------------------------------|---------------------|
| Управление стандартными правилами задачи с помощью Консоли программы ..... | <a href="#">506</a> |
| Добавление правил анализа журналов с помощью Консоли программы .....       | <a href="#">507</a> |

## Управление стандартными правилами задачи с помощью Консоли программы

► Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. Выберите закладку **Стандартные правила**.
5. Снимите или установите флажок **Применять стандартные правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Security для Windows Server применяет эвристический анализатор для обнаружения аномальной активности на защищаемом устройстве.

Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Security для Windows Server применяет стандартные или пользовательские правила для обнаружения аномальной активности.

По умолчанию флажок установлен.

Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.

6. Из списка стандартных правил выберите правила, которые вы хотите применить:
  - Обнаружена возможная попытка взлома пароля с помощью подбора.
  - Обнаружены признаки компрометации журналов Windows.
  - Обнаружена подозрительная активность со стороны новой установленной службы.
  - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
  - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
  - Обнаружены подозрительные изменения привилегированной группы Администраторы.
  - Обнаружена подозрительная активность во время сетевого сеанса входа.

7. Чтобы настроить параметры выбранных правил, выберите закладку **Расширенная**.
8. В разделе **Обработка перебора пароля** укажите количество попыток и промежутки времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
9. В разделе **Сетевой вход** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Security для Windows Server как аномальная активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
  - a. Нажмите на кнопку **Обзор**.
  - b. Выберите пользователя.
  - c. Нажмите на кнопку **ОК**.
 Указанный пользователь будет добавлен в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
  - a. Введите IP-адрес.
  - b. Нажмите на кнопку **Добавить**.
 Указанный IP-адрес будет добавлен в список доверенных.
13. Выберите закладки **Расписание** и **Дополнительно**, чтобы настроить расписание запуска задачи.
14. В окне **Параметры задачи** нажмите на кнопку **ОК**.  
Параметры задачи Анализ журналов будут сохранены.

## Добавление правил анализа журналов с помощью Консоли программы

- *Чтобы добавить и настроить пользовательское правило анализа журналов, выполните следующие действия:*
1. В дереве Консоли программы разверните узел **Диагностика системы**.
  2. Выберите вложенный узел **Анализ журналов**.
  3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.  
Откроется окно **Правила анализа журналов**.
  4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.  
**Контрольная сумма отображается в журнале выполнения задачи.**  
 Если этот флажок установлен, Kaspersky Security для Windows Server применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.  
 Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Security для Windows Server применяет параметры правил по умолчанию.  
 По умолчанию флажок установлен. Активно только правило обнаружения всплывающих окон программ.

Вы можете контролировать применение стандартных правил в задаче Анализ журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать пользовательское правило, выполните следующие действия:
  - a. Введите имя нового правила.
  - b. Нажмите на кнопку **Добавить**.  
Созданное правило добавится в общий список правил.
6. Чтобы настроить любое правило, выполните следующие действия:
  - a. Выберите правило в списке.  
В правой области окна на закладке **Описание** отобразится общая информация о правиле.

Комментарии для нового правила пусты.

- b. Выберите закладку **Описание правила**.
  - c. В разделе **Общие** при необходимости отредактируйте название правила.
  - d. Выберите **Источник**.
7. В разделе **Идентификаторы событий** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
  - a. Укажите идентификатор события.
  - b. Нажмите на кнопку **Добавить**.  
Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
8. Нажмите на кнопку **Сохранить**.  
Настроенные параметры правил анализа журналов будут применены.

## Управление правилами анализа журналов с помощью Веб-плагина

► Чтобы добавить и настроить правила анализа журналов с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Настройка** в подразделе **Анализ журналов**.
6. Настройте параметры, приведены в следующей таблице.

Table 79. Параметры задачи Анализ журналов

| Параметр                                                                                              | Описание                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Применять пользовательские правила для анализа журналов</b>                                        | Пользовательские правила можно включать, отключать, добавлять или изменять.<br>Этот параметр доступен в таблице со списком пользовательских правил.                                                      |
| <b>Использовать стандартные правила для анализа журналов</b>                                          | Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве.<br>Этот параметр доступен в таблице со списком пользовательских правил. |
| <b>Обработка попытки подбора пароля, если неправильный пароль вводится с заданной частотой</b>        | Можно указать количество попыток и промежутков времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.                                             |
| <b>Обработка сетевого входа, если обнаружена попытка входа в течение заданного промежутка времени</b> | Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Security для Windows Server расценивает данное действие как аномальную активность.          |
| <b>Исключение пользователей</b>                                                                       | Можно указать пользователей, которые не будут являться критериями срабатывания эвристического анализатора.                                                                                               |
| <b>Исключить IP-адреса</b>                                                                            | Можно указать IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.                                                                                                   |
| Управление задачами                                                                                   | Вы можете настроить расписание запуска задачи.                                                                                                                                                           |

# Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и по настройке параметров безопасности защищаемого устройства.

## В этом разделе

|                                                                               |                     |
|-------------------------------------------------------------------------------|---------------------|
| О задачах проверки по требованию.....                                         | <a href="#">510</a> |
| Об области проверки и параметрах безопасности задачи .....                    | <a href="#">511</a> |
| Стандартные области проверки .....                                            | <a href="#">512</a> |
| Проверка файлов в облачном хранилище .....                                    | <a href="#">514</a> |
| Стандартные уровни безопасности .....                                         | <a href="#">515</a> |
| Проверка съемных дисков .....                                                 | <a href="#">518</a> |
| О задаче Мониторинг целостности файлов на основе эталона.....                 | <a href="#">519</a> |
| Включение запуска задачи проверки по требованию из контекстного меню .....    | <a href="#">520</a> |
| Заданные по умолчанию параметры задач проверки по требованию .....            | <a href="#">521</a> |
| Управление задачами проверки по требованию с помощью Плагина управления ..... | <a href="#">523</a> |
| Управление задачами проверки по требованию с помощью Консоли программы .....  | <a href="#">541</a> |
| Управление задачами проверки по требованию с помощью Веб-плагина .....        | <a href="#">560</a> |

## О задачах проверки по требованию

Kaspersky Security для Windows Server проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Security для Windows Server проверяет файлы и оперативную память защищаемого устройства, а также объекты автозапуска.

В Kaspersky Security для Windows Server предусмотрены следующие задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Security для Windows Server. Kaspersky Security для Windows Server проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Security для Windows Server создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет их резервными копиями.
- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Security для Windows Server проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы в системных папках, например, в папке %windir%\system32. Kaspersky Security для Windows Server применяет параметры безопасности, соответствующие рекомендуемому уровню (см. раздел "Стандартные уровни безопасности" на стр. [515](#)). Вы можете изменять параметры задачи Проверка важных областей.

- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Security для Windows Server на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом устройстве.

Kaspersky Security для Windows Server может одновременно выполнять несколько задач проверки по требованию.

## Об области проверки и параметрах безопасности задачи

В Консоли программы область проверки выбранной задачи проверки по требованию представляет собой дерево или список файловых ресурсов защищаемого устройства, которые может контролировать Kaspersky Security для Windows Server. По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы включить отображение сетевых файловых ресурсов в виде дерева в Консоли программы,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Параметры области проверки**, выберите элемент **Показывать в виде дерева**.

Элементы и узлы в дереве или списке файловых ресурсов защищаемого устройства отображаются следующим образом:

 Узел включен в область проверки.

 Узел исключен из области проверки.

 – по крайней мере один из узлов, вложенных в этот узел, исключен из области проверки, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок  отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области проверки для выбранного вложенного узла.

С помощью Консоли программы можно также добавлять в область проверки виртуальные диски (см. раздел "Формирование виртуальной области проверки" на стр. 547). Имена виртуальных узлов отображаются шрифтом синего цвета.

## Параметры безопасности

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию параметры безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (**Максимальное быстрое действие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов или элементов в дереве или списке файловых ресурсов защищаемого устройства (уровень безопасности примет значение **Пользовательский**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

## Стандартные области проверки

Дерево или список файловых ресурсов защищаемого устройства для выбранной задачи проверки по требованию отображается в окне **Параметры области проверки**.

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Security для Windows Server предусмотрены следующие стандартные области проверки:

- **Мой компьютер.** Kaspersky Security для Windows Server проверяет защищаемое устройство целиком.
- **Локальные жесткие диски.** Kaspersky Security для Windows Server проверяет объекты на жестких дисках защищаемого устройства. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски.** Kaspersky Security для Windows Server проверяет файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение.** Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, используемая для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются с правами системной учетной записи.



Подключенные сетевые диски также не отображаются в дереве файловых ресурсов защищаемого устройства. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Системная память.** Kaspersky Security для Windows Server проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска.** Kaspersky Security для Windows Server проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули, которые автоматически запускаются при запуске защищаемого устройства.
- **Папки общего доступа.** Вы можете включать в область проверки папки общего доступа на защищаемом устройстве.
- **Виртуальные диски.** Вы можете включать в область проверки виртуальные папки, файлы и диски, подключенные к защищаемому устройству, например, общие диски кластера.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы проверить объекты на виртуальном диске, включите в область проверки папку на защищаемом устройстве, с которой связан этот виртуальный диск.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов. Они доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**
  - **Съемные диски**
  - **Системная память**
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
- Прочие задачи:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
  - **Папки общего доступа**

## Проверка файлов в облачном хранилище

### Об облачных файлах

Kaspersky Security для Windows Server может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы из OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Security для Windows Server не поддерживает другие облачные хранилища.

Функция "файлы из OneDrive по запросу" помогает получить доступ к вашим файлам OneDrive без необходимости загружать их и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы из OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

 — этот значок показывает, что файл *доступен только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, вы не сможете открывать файлы, доступные только через интернет.

 — этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ().

 — этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

### Проверка облачных файлов

Kaspersky Security для Windows Server может выполнять проверку только облачных файлов, сохраненных локально на защищаемом устройстве. Такие файлы OneDrive имеют статус  или . Проверка файлов со статусом  не выполняется, поскольку физически они не хранятся на защищаемом устройстве.

Во время проверки Kaspersky Security для Windows Server не выполняет автоматическую загрузку файлов со статусом  из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Security для Windows Server в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область задачи Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан задачей Постоянная защита файлов.
- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами  и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано

информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.

- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами  и  с помощью задачи Формирование правил контроля запуска программ. Задача Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

Задача Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом  не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

## Стандартные уровни безопасности

Параметры безопасности **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** не входят в набор параметров стандартных уровней безопасности. При изменении параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов**, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов узла можно задать один из трех стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свои стандартные параметры безопасности (см. таблицу ниже).

### Максимальное быстроедействие

Уровень безопасности **Максимальное быстроедействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Security для Windows Server на защищаемых устройствах и рабочих станциях, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

### Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности устройств в сети организации.

Table 80. Стандартные уровни безопасности и соответствующие им значения

| Параметры                                                  | Уровень безопасности                                                                                                                                                 |                                                                                                                                                                           |                                                                                                                                                                                                                                         |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | Максимально<br>е<br>быстродействие                                                                                                                                   | Рекомендуемый                                                                                                                                                             | Максимальная защита                                                                                                                                                                                                                     |
| Проверка объектов                                          | По формату                                                                                                                                                           | Все объекты                                                                                                                                                               | Все объекты                                                                                                                                                                                                                             |
| Проверять только новые и измененные файлы                  | Включена                                                                                                                                                             | Выключено                                                                                                                                                                 | Выключено                                                                                                                                                                                                                               |
| Действия над зараженными и другими обнаруженными объектами | Лечить.<br>Удалить, если не удалось вылечить.                                                                                                                        | Выполнять рекомендованное действие (Лечить. Удалить, если не удалось вылечить.)                                                                                           | Лечить.<br>Удалить, если не удалось вылечить.                                                                                                                                                                                           |
| Действия над возможно зараженными объектами                | Карантин                                                                                                                                                             | Выполнять рекомендованное действие (Поместить на карантин)                                                                                                                | Карантин                                                                                                                                                                                                                                |
| Исключать файлы                                            | Нет                                                                                                                                                                  | Нет                                                                                                                                                                       | Нет                                                                                                                                                                                                                                     |
| Не обнаруживать                                            | Нет                                                                                                                                                                  | Нет                                                                                                                                                                       | Нет                                                                                                                                                                                                                                     |
| Останавливать проверку, если она длится более (сек)        | 60 сек.                                                                                                                                                              | Нет                                                                                                                                                                       | Нет                                                                                                                                                                                                                                     |
| Не проверять составные объекты размером более (МБ)         | 8 МБ                                                                                                                                                                 | Нет                                                                                                                                                                       | Нет                                                                                                                                                                                                                                     |
| Альтернативные потоки NTFS                                 | Да                                                                                                                                                                   | Да                                                                                                                                                                        | Да                                                                                                                                                                                                                                      |
| Проверять загрузочные секторы дисков и MBR                 | Да                                                                                                                                                                   | Да                                                                                                                                                                        | Да                                                                                                                                                                                                                                      |
| Проверять составные объекты                                | <ul style="list-style-type: none"> <li>• SFX-архивы*</li> <li>• Упакованные объекты*</li> <li>• Вложенные OLE-объекты*</li> </ul> <p>* Только новые и измененные</p> | <ul style="list-style-type: none"> <li>• Архивы*</li> <li>• SFX-архивы*</li> <li>• Упакованные объекты*</li> <li>• Вложенные OLE-объекты*</li> </ul> <p>* Все объекты</p> | <ul style="list-style-type: none"> <li>• Архивы*</li> <li>• SFX-архивы*</li> <li>• Почтовые базы*</li> <li>• Файлы почтовых форматов*</li> <li>• Упакованные объекты*</li> <li>• Вложенные OLE-объекты*</li> </ul> <p>* Все объекты</p> |

## Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.

Kaspersky Security для Windows Server выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу проверки по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Kaspersky Security для Windows Server не блокирует доступ к съемному диску на время проверки.

Результаты проверки каждого съемного диска доступны в журнале выполнения задачи проверки по требованию, созданной при подключении этого съемного диска.

Вы можете изменять значения параметров компонента Проверка съемных дисков (см. таблицу ниже).

Table 81. Параметры проверки съемных дисков

| Параметр                                                                          | Значение по умолчанию | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Проверять съемные диски при их подключении по USB</b>                          | Флажок снят           | Вы можете включать или выключать проверку съемных дисков при их подключении к защищаемому устройству по USB.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Проверять, если объем содержащихся на диске данных не превышает порог (МБ)</b> | 1024 МБ               | Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на проверяемом диске.<br><br>Kaspersky Security для Windows Server не выполняет проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение.                                                                                                                                                                                                                                                         |
| <b>Запускать проверку с уровнем безопасности</b>                                  | Максимальная защита   | Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: <ul style="list-style-type: none"> <li>• <b>Максимальная защита</b></li> <li>• <b>Рекомендуемый</b></li> <li>• <b>Максимальное быстроедействие</b></li> </ul> Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию. |

## О задаче Мониторинг целостности файлов на основе эталона

Во время выполнения задачи Мониторинг целостности файлов на основе эталона Kaspersky Security для Windows Server не проверяет заблокированные файлы, папки, ярлыки файлов и облачные файлы.

В задаче Мониторинг целостности файлов на основе эталона выполняется контроль целостности файлов в области мониторинга посредством сравнения хеша файлов (MD5 или SHA256) с эталонным значением.

При первом запуске задачи Мониторинг целостности файлов на основе эталона, Kaspersky Security для Windows Server создает эталон, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При изменении области задачи Мониторинг целостности файлов на основе эталона, Kaspersky Security для Windows Server обновляет эталон при следующем запуске задачи Мониторинг целостности файлов на основе эталона, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При удалении задачи Мониторинг целостности файлов на основе эталона, Kaspersky Security для Windows Server удаляет эталон этой задачи.

С помощью командной строки можно удалить эталон (см. раздел "Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE" на стр. [722](#)), не удаляя задачу Мониторинг целостности файлов на основе эталона.

Задача Мониторинг целостности файлов на основе эталона отслеживает следующие изменения файлов в области мониторинга:

- область мониторинга содержит файл, который отсутствует в эталоне;
- в области мониторинга отсутствует файл, который присутствует в эталоне;
- хеш файла в области мониторинга отличается от хеша этого файла в эталоне.

Задача Мониторинг целостности файлов на основе эталона не отслеживает изменения атрибутов файлов и изменения альтернативных потоков.

Если файл или папка недоступны, Kaspersky Security для Windows Server не добавляет этот файл или папку в эталон при создании, а формирует событие о невозможности рассчитать хеш при запуске задачи Мониторинг целостности файлов на основе эталона.

Файл или папка могут быть недоступны по следующим причинам:

- указанный путь не существует;
- тип файлов, указанный в маске, отсутствует по указанному пути;
- указанный файл заблокирован;
- указан пустой файл.

## Включение запуска задачи проверки по требованию из контекстного меню

Можно включить запуск задачи проверки по требованию из контекстного меню файла в проводнике Windows.

► Чтобы включить запуск задачи проверки по требованию из контекстного меню, выполните следующие действия:

### 1. Создайте следующие REG-файлы:

```
Windows Registry Editor Version 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\ksws\command]
@="C:\\Temp\\scan.cmd \"%1\""
```

```
[HKEY_CLASSES_ROOT\\*\\shell\\ksws\\command]
@="C:\\Temp\\scan.cmd \"%1\""
```

```
[HKEY_CLASSES_ROOT\\Directory\\shell\\ksws]
@="Проверить с помощью Kaspersky Security"
```

```
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Security for Windows Server\\kavtrayr.dll\",0"
```

```
[HKEY_CLASSES_ROOT\\Directory\\shell\\ksws\\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Security for Windows Server\\kavtrayr.dll\",0"
```

```
[HKEY_CLASSES_ROOT\\*\\shell\\ksws]
@="Проверить с помощью Kaspersky Security"
```

```
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Security for Windows Server\\kavtrayr.dll\",0"
```

```
[HKEY_CLASSES_ROOT\\*\\shell\\ksws\\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Security for Windows Server\\kavtrayr.dll\",0"
```

```
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\AppCompatFlags\\Layers]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Security for Windows Server\\kavtrayr.dll\",0"
```

Необходимо указать реальное местоположение папки, в которую установлена программа Kaspersky Security для Windows Server.

### 2. Создайте файл scan.cmd со следующим содержимым:

```
@echo off
set LOGNAME=%RANDOM%
```



```
"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security for Windows
Server\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt
```

```
echo Выполняется проверка...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

Файл `scan.cmd` должен содержать следующую информацию:

- Местоположение файла `kavshell.exe`.
  - Местоположение временного файла, содержащего результаты проверки.
  - Параметры команды `KAVSHELL SCAN`.
  - Значение времени ожидания закрытия окна консоли после завершения задачи.
3. Скопируйте файл `scan.cmd` в папку, указанную в REG-файле как значение параметра `[HKEY_CLASSES_ROOT\Directory\shell\ksws\command]`.

В примере указана папка `C:\Temp`.

Перезагрузка операционной системы не требуется.

## Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Table 82. Заданные по умолчанию параметры задач проверки по требованию

| Параметр         | Значение по умолчанию                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Описание                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Область проверки | <p>Применяется в следующих системных и пользовательских задачах:</p> <ul style="list-style-type: none"> <li>• <b>Проверка при старте операционной системы:</b> защищаемое устройство целиком, за исключением папок общего доступа и объектов автозапуска.</li> <li>• <b>Проверка важных областей:</b> защищаемое устройство целиком, за исключением папок общего доступа и некоторых файлов операционной системы.</li> <li>• <b>Проверка по требованию</b></li> </ul> | <p>Вы можете изменить область проверки. Область проверки нельзя настроить для системных задач <b>Проверка объектов на карантине</b> и <b>Проверка целостности программы</b>.</p> |

| Параметр                                                    | Значение по умолчанию                                                                                                                                                                                                                                       | Описание                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             | (пользовательские задачи):<br>защищаемое устройство целиком.                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                           |
| Параметры безопасности                                      | Единые для всей области проверки, соответствуют уровню безопасности <b>Рекомендуемый</b> .                                                                                                                                                                  | Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: <ul style="list-style-type: none"> <li>• выбрать другой стандартный уровень безопасности;</li> <li>• вручную изменить параметры безопасности.</li> </ul> Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла. |
| <b>Использование эвристического анализатора</b>             | Применяется с уровнем анализа <b>Средний</b> для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач.<br>Применяется с уровнем анализа <b>Глубокий</b> для задачи Проверка объектов на карантине. | Вы можете включать и выключать применение эвристического анализатора и регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине.<br>Эвристический анализатор не используется в задачах Проверка целостности программы и Мониторинг целостности файлов на основе эталона.                                                                            |
| <b>Применять доверенную зону</b>                            | Применяется (не применяется для задачи Проверка объектов на карантине)                                                                                                                                                                                      | Единый список исключений, который можно применять в выбранных задачах.                                                                                                                                                                                                                                                                                                                                    |
| <b>Использовать KSN для проверки</b>                        | Применяется.                                                                                                                                                                                                                                                | Вы можете увеличить эффективность защиты устройства с помощью инфраструктуры облачных служб Kaspersky Security Network.                                                                                                                                                                                                                                                                                   |
| Параметры запуска задачи с определенными правами            | Задача запускается с правами системной учетной записи.                                                                                                                                                                                                      | Вы можете изменять параметры запуска задач с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.                                                                                                                                                                                     |
| <b>Выполнять задачу в фоновом режиме</b> (низкий приоритет) | Не применяется                                                                                                                                                                                                                                              | Вы можете настраивать приоритетность выполнения задач проверки по требованию.                                                                                                                                                                                                                                                                                                                             |

| Параметр                                                               | Значение по умолчанию                                                                                                                                                                                                                                                                                                                                                                                                                              | Описание                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Расписание запуска задачи                                              | <p>Применяется в системных задачах:</p> <ul style="list-style-type: none"> <li>• Проверка при старте операционной системы – <b>При запуске программы</b>;</li> <li>• Проверка важных областей – <b>Еженедельно</b>;</li> <li>• Проверка объектов на карантине – <b>После обновления баз программы</b>;</li> <li>• Проверка целостности программы – <b>Ежедневно</b>.</li> </ul> <p>Не применяется во вновь созданных пользовательских задачах.</p> | Можно настроить параметры для запуска задачи по расписанию.                                                                                                                                                                                                                                                                                                                     |
| Регистрация выполнения проверки и обновление статуса защиты устройства | Статус защиты устройства обновляется еженедельно после выполнения задачи Проверка важных областей.                                                                                                                                                                                                                                                                                                                                                 | <p>Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами:</p> <ul style="list-style-type: none"> <li>• изменяя параметры расписания запуска задачи Проверка важных областей;</li> <li>• изменяя область проверки задачи Проверка важных областей;</li> <li>• создавая пользовательские задачи проверки по требованию.</li> </ul> |

## Управление задачами проверки по требованию с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

### В этом разделе

|                                                                               |                     |
|-------------------------------------------------------------------------------|---------------------|
| Навигация .....                                                               | <a href="#">524</a> |
| Создание задачи проверки по требованию .....                                  | <a href="#">525</a> |
| Настройка области проверки для задачи .....                                   | <a href="#">530</a> |
| Выбор стандартных уровней безопасности в задачах проверки по требованию ..... | <a href="#">531</a> |
| Настройка параметров безопасности вручную .....                               | <a href="#">532</a> |
| Настройка проверки съемных дисков .....                                       | <a href="#">539</a> |
| Настройка задачи Мониторинг целостности файлов на основе эталона .....        | <a href="#">540</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                                |                     |
|----------------------------------------------------------------|---------------------|
| Переход к мастеру создания задачи проверки по требованию ..... | <a href="#">524</a> |
| Переход к свойствам задачи проверки по требованию .....        | <a href="#">525</a> |

## Переход к мастеру создания задачи проверки по требованию

► Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:

1. Для создания локальной задачи:
  - a. Разверните узел **Управляемые устройства** в Консоли администрирования Kaspersky Security Center.
  - b. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
  - c. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства.
  - d. Выберите пункт меню **Свойства**.
  - e. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.Откроется окно **Мастер создания задачи**.
2. Для создания групповой задачи:
  - a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  - b. Выберите группу администрирования, для которой требуется создать задачу.
  - c. Выберите закладку **Задачи**.
  - d. Нажмите на кнопку **Создать задачу**.Откроется окно **Мастер создания задачи**.
3. Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
  - a. В Консоли администрирования Kaspersky Security Center в панели результатов узла **Выборки устройств** нажмите на кнопку **Запустить выборку**, чтобы выбрать устройства.
  - b. Выберите закладку **Результаты выборки "имя выборки"**.
  - c. В раскрывающемся списке **Сделать выборку** выберите вариант **Создать задачу для результатов выборки**.Откроется окно **Мастер создания задачи**.
4. Выберите задачу **Проверка по требованию** в списке доступных задач для Kaspersky Security для Windows Server.

5. Нажмите на кнопку **Далее**.

Откроется окно **Параметры**.

Настройте параметры задачи в соответствии с вашими требованиями.

- *Чтобы настроить задачу проверки по требованию,*

откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач Kaspersky Security Center.

Откроется окно **Свойства: Проверка по требованию**.

## Переход к свойствам задачи проверки по требованию

- *Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите закладку **Устройства**.
4. Дважды щелкните мышью по имени защищаемого устройства, для которого вы хотите настроить область проверки.

Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. Выберите раздел **Задачи**.
6. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
7. Нажмите на кнопку **Свойства**.

Откроется окно **Свойства: Проверка по требованию**.

Настройте параметры задачи в соответствии с вашими требованиями.

## Создание задачи проверки по требованию

- *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Откройте окно **Параметры** (см. раздел "Переход к мастеру создания задачи проверки по требованию" на стр. [524](#)) в мастере создания задачи.
2. Выберите требуемый **Способ создания задачи**.
3. Нажмите на кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки.

По умолчанию область проверки включает критические области защищаемого устройства. Проверяемые области помечены в таблице значком . Области, являющиеся исключениями из проверки, помечены в таблице значком .

Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

- Чтобы исключить из проверки все важные области, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
- Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
  - a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить область** или нажмите на кнопку **Добавить**.
  - b. В окне **Добавление в область проверки** выберите стандартную область в списке **Стандартная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом устройстве в сети и нажмите на кнопку **ОК**.
- Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:
  - a. Откройте контекстное меню и выберите пункт **Настроить**.
  - b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
  - c. На закладке **Общие** в окне **Параметры проверки по требованию** снимите флажки **Вложенные папки** и **Вложенные файлы**.
- Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
  - a. Откройте контекстное меню области проверки, параметры которой требуется изменить, и выберите пункт **Настроить**.
  - b. В окне **Параметры проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

Параметры безопасности настраиваются таким же образом, как и для задачи **Постоянная защита файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. [310](#)).

- Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:
    - a. Откройте контекстное меню таблицы **Область проверки** и выберите пункт **Добавить исключение**.
    - b. Укажите объекты, которые вы хотите исключить: выберите стандартную область в списке **Стандартная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом устройстве в сети.
    - c. Нажмите на кнопку **ОК**.
5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:
- Настройте использование эвристического анализатора (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. [305](#)).
  - Установите флажок **Применять доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

- Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

Этот флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача проверки по требованию не использует службы KSN.

По умолчанию флажок установлен.

- Чтобы присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**.

Флажок изменяет приоритет задачи.

Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Security для Windows Server и программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Security для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

По умолчанию флажок снят.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Security для Windows Server, имеют приоритет *Средний*.

- Чтобы использовать создаваемую задачу в качестве задачи Проверка важных областей, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых устройств по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Security для Windows Server. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

Если флажок снят, задача выполняется с низким приоритетом.

По умолчанию флажок снят для пользовательских задач проверки по требованию.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** укажите параметры запуска задачи по расписанию.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
10. Нажмите на кнопку **Далее**.
11. Укажите название задачи.
12. Нажмите на кнопку **Далее**.

Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " \* < > & \ : |

Откроется окно **Завершение создания задачи**.

13. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
14. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача проверки по требованию для выбранного защищаемого устройства или группы защищаемых устройств.

## В этом разделе

|                                                                                 |                     |
|---------------------------------------------------------------------------------|---------------------|
| Присвоение задаче проверки по требованию статуса Проверка важных областей ..... | <a href="#">528</a> |
| Выполнение задач проверки по требованию в фоновом режиме .....                  | <a href="#">529</a> |
| Регистрация выполнения задачи Проверка важных областей.....                     | <a href="#">530</a> |

## Присвоение задаче проверки по требованию статуса Проверка важных областей

По умолчанию Kaspersky Security Center присваивает защищаемому устройству статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано параметром для порога формирования события в Kaspersky Security для Windows Server – *Проверка важных областей не проводилась давно*.

► Чтобы настроить проверку всех защищаемых устройств, входящих в одну группу администрирования, выполните следующие действия:

1. Создайте групповую задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. [525](#)).
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей**. Указанные параметры задачи (область проверки и параметры безопасности) будут применены ко всем защищаемым устройствам в группе. Настройте расписание задачи.



Флажок **Считать выполнение задачи проверкой важных областей** можно установить при создании задачи проверки по требованию для группы защищаемых устройств или позднее в окне **Свойства: <Название задачи>** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. [525](#)).

3. С помощью новой или существующей политики выключите запуск по расписанию системных задач проверки по требованию для группы защищаемых устройств (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [110](#)).

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого устройства и уведомлять о нем по результатам последнего выполнения задачи со статусом Проверка важных областей, а не по результатам выполнения системной задачи Проверка важных областей.

Вы можете присваивать статус *Проверка важных областей* как групповым задачам проверки по требованию, так и задачам для групп защищаемых устройств.

В Консоли программы можно также просмотреть, имеет ли задача проверки по требованию статус Проверка важных областей.

В Консоли программы флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задачи, но не доступен для редактирования.

## Выполнение задач проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Security для Windows Server, имеют приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но может положительно повлиять на скорость выполнения процессов других запущенных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Можно указать максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к мастеру создания задачи проверки по требованию" на стр. [524](#)).
2. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

Флажок изменяет приоритет задачи.

Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Security для Windows Server и программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

Если флажок снят, задача выполняется с тем же приоритетом, что и остальные

задачи Kaspersky Security для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

По умолчанию флажок снят.

3. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

## Регистрация выполнения задачи Проверка важных областей

По умолчанию статус защиты устройства отображается в панели результатов узла **Kaspersky Security** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты устройства привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. По умолчанию флажок установлен только для задачи Проверка важных областей и недоступен для редактирования в этой задаче.

Вы можете выбрать задачу проверки по требованию, связанную со статусом защиты устройства, только в Kaspersky Security Center.

## Настройка области проверки для задачи

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Security для Windows Server (**Пуск > Программы > Kaspersky Security для Windows Server > Изменить или удалить**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры программы**.

► Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. Чтобы включить элементы в область проверки:
  - a. Откройте контекстное меню для списка областей проверки.
  - b. В контекстном меню выберите пункт **Добавить область**.
  - c. В открывшемся окне **Добавление в область проверки** выберите тип объектов, который вы хотите добавить:
    - **Стандартная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
    - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.

- **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.

4. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
  - a. Откройте контекстное меню области проверки по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить исключение**.
  - c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
5. Чтобы изменить область проверки или исключение, в контекстном меню требуемой области проверки выберите пункт **Изменить область**.
6. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

7. Нажмите на кнопку **ОК**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

## Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узлов, выбранных в списке файловых ресурсов защищаемого устройства, можно задать один из трех стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** и **Максимальная защита**.

► Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. В списке защищаемых устройств выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

Откроется окно **Параметры проверки по требованию**.

5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

6. Нажмите на кнопку **ОК**.
7. В окне **Свойства: Проверка по требованию** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

## Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. В списке областей проверки выберите элементы, для которых вы хотите настроить параметры безопасности.

Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. [169](#)) можно применить к выбранному узлу или элементу в области проверки.

4. Нажмите на кнопку **Настроить**.  
Откроется окно **Параметры проверки по требованию**.
  5. На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
    - **Общие** (см. раздел "Настройка общих параметров задачи" на стр. [533](#))
    - **Действия** (см. раздел "Настройка действий" на стр. [536](#))
    - **Производительность** (см. раздел "Настройка производительности" на стр. [538](#))
    - **Иерархическое хранилище**
  6. Нажмите на кнопку **ОК** в окне **Параметры проверки по требованию**.
  7. Нажмите на кнопку **ОК** в окне **Область проверки**.
- Новые параметры области проверки будут сохранены.

## В этом разделе

|                                         |                     |
|-----------------------------------------|---------------------|
| Настройка общих параметров задачи ..... | <a href="#">533</a> |
| Настройка действий.....                 | <a href="#">536</a> |
| Настройка производительности .....      | <a href="#">538</a> |

## Настройка общих параметров задачи

► Чтобы настроить общие параметры задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.  
Откроется окно **Параметры проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. На закладке **Общие** в блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:

- **Проверяемые объекты:**

- **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Вложенные папки**

- **Вложенные файлы**

- **Проверять загрузочные секторы дисков и MBR**

Включение защиты загрузочных секторов дисков и основных загрузочных записей.

Если флажок установлен, Kaspersky Security для Windows Server проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

По умолчанию флажок установлен.

6. В блоке параметров **Производительность** установите или снимите флажок **Проверять только новые и измененные файлы**.

Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Security для Windows Server новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет и защищает файлы, независимо от того, когда они были изменены.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстрое действие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все / Только новые** для каждого типа составных объектов.

7. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Все / Только новые архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

Проверка файлов почтовых баз Microsoft Outlook® и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

8. Нажмите на кнопку **ОК**.

Новая конфигурация задачи будет сохранена.



## Настройка действий

► Чтобы настроить действия над зараженными и другими обнаруженными объектами во время выполнения задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.  
Откроется окно **Параметры проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Действия**.
6. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Лечить**
- **Лечить. Удалять, если не удалось вылечить**
- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Выполнять рекомендуемое действие**

7. Выберите действие над возможно зараженными объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Помещать на карантин**



- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Выполнять рекомендуемое действие**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

- a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Security для Windows Server не позволит открыть или запустить зараженный объект независимо от вашего выбора.

Если флажок снят, Kaspersky Security для Windows Server выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.

- b. Нажмите на кнопку **Настройка**.

- c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

- d. Нажмите на кнопку **ОК**.

2. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

3. Нажмите на кнопку **ОК**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

► Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. [525](#)).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.  
Откроется окно **Параметры проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Производительность**.
6. В блоке **Исключения**:

- Снимите или установите флажок **Исключать файлы**.

Исключение файлов из проверки по имени файла или маске имени файла.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server проверяет все объекты.

По умолчанию флажок снят.

- Снимите или установите флажок **Не обнаруживать**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

7. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстрое действие**.

- **Не проверять составные объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

Если флажок снят, Kaspersky Security для Windows Server проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстроедействие**.

- **Использовать технологию iSwift**

iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Security для Windows Server проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

По умолчанию флажок установлен.

- **Использовать технологию iChecker**

iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Security для Windows Server проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

8. Нажмите на кнопку **ОК**.

Новая конфигурация задачи будет сохранена.

## Настройка проверки съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительно**.

5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

Откроется окно **Проверка съемных дисков**.

6. В блоке **Проверка при подключении** выполните следующие действия:
  - Установите флажок **Проверять съемные диски при подключении по USB**, если вы хотите, чтобы программа Kaspersky Security для Windows Server автоматически выполняла проверку съемных дисков при их подключении.
  - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
  - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.
7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

## Настройка задачи Мониторинг целостности файлов на основе эталона

- *Чтобы настроить групповую задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
  - Выберите название задачи в списке созданных задач двойным щелчком мыши.
  - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
  - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.

В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

4. В разделе **Область мониторинга** выполните следующие действия:
  - а. Чтобы добавить папку в область задачи Мониторинг целостности файлов на основе эталона:
    1. Нажмите на кнопку **Добавить**.  
Откроется окно **Параметры области мониторинга**.
    2. Установите или снимите флажок **Контролировать эту область**.
    3. Нажмите на кнопку **Обзор**, чтобы указать папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
    4. Установите флажок **Контролировать вложенные папки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.

- b. Чтобы добавить или исключить добавленную ранее папку из области задачи Мониторинг целостности файлов на основе эталона, снимите или установите флажок слева от пути к папке в таблице **Область мониторинга**.
- c. Чтобы удалить папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите папку в таблице **Область мониторинга** и нажмите на кнопку **Удалить**.
- 5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
- 6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
- 7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в [Справке Kaspersky Security Center](#).

- 8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.  
Настроенные параметры групповых задач будут сохранены.

## Управление задачами проверки по требованию с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

### В этом разделе

|                                                                                   |                     |
|-----------------------------------------------------------------------------------|---------------------|
| Навигация .....                                                                   | <a href="#">541</a> |
| Создание и настройка задачи проверки по требованию .....                          | <a href="#">542</a> |
| Область проверки в задачах проверки по требованию .....                           | <a href="#">544</a> |
| Настройка параметров безопасности .....                                           | <a href="#">548</a> |
| Проверка съемных дисков .....                                                     | <a href="#">556</a> |
| Статистика задач проверки по требованию .....                                     | <a href="#">557</a> |
| Создание и настройка задачи Мониторинг целостности файлов на основе эталона ..... | <a href="#">559</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

## В этом разделе

|                                                                           |                     |
|---------------------------------------------------------------------------|---------------------|
| Переход к параметрам задачи проверки по требованию .....                  | <a href="#">542</a> |
| Переход к параметрам области действия задачи проверки по требованию ..... | <a href="#">542</a> |

## Переход к параметрам задачи проверки по требованию

- Чтобы перейти к общим параметрам задачи проверки по требованию в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

## Переход к параметрам области действия задачи проверки по требованию

- Чтобы перейти к параметрам области проверки в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

Откроется окно **Параметры области проверки**.

## Создание и настройка задачи проверки по требованию

Вы можете создавать пользовательские задачи для отдельного защищаемого устройства в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Security для Windows Server создание пользовательских задач не предусмотрено.

- Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

Откроется окно **Добавить задачу**.

3. Настройте следующие параметры задачи:

- **Имя** – название задачи, содержащее не более 100 символов. Допускаются любые символы, кроме " \* < > & \ : |.

Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано название задачи.

- **Описание** – дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.
- **Использование эвристического анализатора**

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.
- **Выполнять задачу в фоновом режиме**

Флажок изменяет приоритет задачи.

Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Security для Windows Server и программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Security для Windows Server и другие программы. В этом случае скорость выполнения задачи увеличивается.

По умолчанию флажок снят.
- **Применять доверенную зону**

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.
- **Считать выполнение задачи проверкой важных областей**

Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых устройств по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Security для Windows Server. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

Если флажок снят, задача выполняется с низким приоритетом.

По умолчанию флажок снят для пользовательских задач проверки по требованию.

- **Использовать KSN для проверки**

Этот флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача проверки по требованию не использует службы KSN.

По умолчанию флажок установлен.

4. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)) на вкладках **Расписание** и **Дополнительно**.
5. На вкладке **Запуск с правами** настройте запуск задачи с правами определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)).
6. В окне **Добавить задачу** нажмите на кнопку **ОК**.  
Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (стр. [247](#)).
7. Если требуется, в панели результатов выбранного узла выберите **Настройка области проверки**.  
Откроется окно **Параметры области проверки**.
8. В дереве или в списке файловых ресурсов защищаемого устройства выберите узлы или элементы, которые вы хотите включить в область проверки.
9. Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. [515](#)) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности" на стр. [548](#)).
10. Нажмите на кнопку **Сохранить** в окне **Параметры области проверки**.  
Настроенные параметры будут применены при последующем запуске задачи.

## Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

### В этом разделе

|                                                       |                     |
|-------------------------------------------------------|---------------------|
| Настройка отображения сетевых файловых ресурсов ..... | <a href="#">545</a> |
| Формирование области проверки .....                   | <a href="#">545</a> |
| Включение в область проверки сетевых объектов.....    | <a href="#">547</a> |
| Создание виртуальной области проверки.....            | <a href="#">547</a> |



## Настройка отображения сетевых файловых ресурсов

► Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области проверки, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
  - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
  - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

3. Нажмите на кнопку **Сохранить**.

## Формирование области проверки

Если вы управляете Kaspersky Security для Windows Server на защищаемом устройстве удаленно, с помощью Консоли программы, установленной на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом устройстве, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Security для Windows Server (**Пуск > Программы > Kaspersky Security для Windows Server > Изменить или удалить**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от выбранного типа отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. [545](#)). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

► Чтобы сформировать область проверки с помощью дерева сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
  - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.

- Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
  - Если вы хотите включить в область проверки все диски определенного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски защищаемого устройства, установите флажок **Съемные диски**).
  - Если вы хотите включить в область проверки отдельный диск определенного типа, разверните узел, который содержит диски этого типа, и установите флажок рядом с именем требуемого диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
  - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.

4. Нажмите на кнопку **Сохранить**.

Окно **Параметры области проверки** будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область проверки с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).
2. Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
  - a. Откройте контекстное меню области проверки по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить область проверки**.
  - c. В открывшемся окне **Добавить область проверки** выберите тип объектов, который вы хотите добавить:
    - **Стандартная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
    - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
    - **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.

3. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
  - a. Откройте контекстное меню области проверки по правой клавише мыши.
  - b. В контекстном меню выберите пункт **Добавить исключение**.
  - c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
4. Чтобы изменить добавленную область проверки или исключение, в контекстном меню нужной области проверки выберите пункт **Изменить область**.

5. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

6. Нажмите на кнопку **Сохранить**.

Окно **Параметры области проверки** будет закрыто. Настроенные параметры задачи будут сохранены.

## Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► Чтобы включить в область проверки сетевой объект, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
  - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
  - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
5. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Создание виртуальной области проверки

Можно включать в область проверки виртуальные диски, папки и файлы, таким образом создавая виртуальную область проверки.

Вы можете включить в область проверки отдельные виртуальные диски, папки или файлы, только если область проверки отображается в виде дерева файловых ресурсов (см. раздел "**Настройка отображения сетевых файловых ресурсов**" на стр. [545](#)).

► Чтобы включить в область проверки виртуальный диск, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла **Виртуальные диски**, выберите пункт **Добавить виртуальный диск** и в списке доступных имен выберите имя виртуального диска.
4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
5. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► Чтобы включить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла, в который вы хотите добавить папку или файл, и выберите один из следующих вариантов:
  - **Добавить виртуальную папку**, если вы хотите добавить виртуальную папку в область проверки.
  - **Добавить виртуальный файл**, если вы хотите добавить виртуальный файл в область проверки.
4. В поле ввода задайте имя для папки или файла.
5. В строке с именем папки или файла установите флажок, чтобы включить папку или файл в область проверки.
6. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Настройка параметров безопасности

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

При работе с деревом сетевых файловых ресурсов параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).

2. В левой части окна выберите узел или элемент, параметры безопасности которого вы хотите настроить.

Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. [169](#)) можно применить к выбранному узлу или элементу в области проверки.

В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. [545](#)), создать область проверки (см. раздел "Формирование области проверки" на стр. [545](#)) и создать виртуальную область проверки (см. раздел "Формирование виртуальной области проверки" на стр. [547](#)).

3. В правой части окна выполните одно из следующих действий:

- На закладке **Уровень безопасности** выберите уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задачах проверки по требованию" на стр. [549](#)).
- На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
  - **Общие** (см. раздел "Настройка общих параметров задачи" на стр. [550](#))
  - **Действия** (см. раздел "Настройка действий" на стр. [552](#))
  - **Производительность** (см. раздел "Настройка производительности" на стр. [554](#))
  - **Иерархическое хранилище**

4. Нажмите на кнопку **Сохранить** в окне **Параметры области проверки**.

Новые параметры области проверки будут сохранены.

## В этом разделе

|                                                                               |                     |
|-------------------------------------------------------------------------------|---------------------|
| Выбор стандартных уровней безопасности в задачах проверки по требованию ..... | <a href="#">549</a> |
| Настройка общих параметров задачи .....                                       | <a href="#">550</a> |
| Настройка действий.....                                                       | <a href="#">552</a> |
| Настройка производительности .....                                            | <a href="#">554</a> |
| Настройка иерархического хранилища.....                                       | <a href="#">556</a> |

## Выбор стандартных уровней безопасности в задачах проверки по требованию

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстрое действие**, **Рекомендуемый** и **Максимальная защита**.

► Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).

2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область проверки.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.

5. Нажмите на кнопку **Сохранить**.

Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

## Настройка общих параметров задачи

► Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "Переход к параметрам области действия задачи проверки по требованию" на стр. [542](#)).
2. Выберите закладку **Общие**.
3. В блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:

- **Проверяемые объекты:**

- **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Проверять загрузочные секторы дисков и MBR**

Включение защиты загрузочных секторов дисков и основных загрузочных записей.

Если флажок установлен, Kaspersky Security для Windows Server проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках

защищаемого устройства.

По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

По умолчанию флажок установлен.

4. В блоке параметров **Производительность** установите или снимите флажок **Проверять только новые и измененные файлы**.

Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Security для Windows Server новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Security для Windows Server проверяет и защищает файлы, независимо от того, когда они были изменены.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все / Только новые** для каждого типа составных объектов.

5. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Все / Только новые архивы**

Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

Проверка самораспаковывающихся архивов.

Если флажок установлен, Kaspersky Security для Windows Server проверяет SFX-архивы.

Если флажок снят, Kaspersky Security для Windows Server пропускает SFX-архивы при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.



Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

Проверка файлов почтовых баз Microsoft Outlook® и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

Если флажок установлен, Kaspersky Security для Windows Server проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Security для Windows Server при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Security для Windows Server проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Security для Windows Server пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

Если флажок установлен, Kaspersky Security для Windows Server проверяет объекты, встроенные в файлы.

Если флажок не установлен, Kaspersky Security для Windows Server пропускает объекты, встроенные в файлы, при проверке.

Значение по умолчанию зависит от выбранного уровня защиты.

## 6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

► Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).



2. Выберите закладку **Действия**.

3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Лечить**

- **Лечить. Удалять, если не удалось вылечить**

- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Выполнять рекомендуемое действие**

4. Выберите действие над возможно зараженными объектами:

- **Только сообщать**

Если выбран этот режим, Kaspersky Security для Windows Server не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта*. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если выбран этот режим, Kaspersky Security для Windows Server автоматически изменит уровень безопасности на **Пользовательский**.

- **Помещать на карантин**

- **Удалять**

Kaspersky Security для Windows Server удаляет объект и помещает его копию в резервное хранилище.

- **Выполнять рекомендуемое действие**

Kaspersky Security для Windows Server выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

а. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка**

рядом с флажком. Однако Kaspersky Security для Windows Server не позволит открыть или запустить зараженный объект независимо от вашего выбора.

Если флажок снят, Kaspersky Security для Windows Server выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.

- b. Нажмите на кнопку **Настройка**.
  - c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
  - d. Нажмите на кнопку **ОК**.
2. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

3. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
  - Снимите или установите флажок **Исключать файлы**.

Исключение файлов из проверки по имени файла или маске имени файла.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server проверяет все объекты.

По умолчанию флажок снят.

- Снимите или установите флажок **Не обнаруживать**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

#### 4. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек)**

Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

Если флажок снят, продолжительность проверки не ограничена.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстроедействие**.

- **Не проверять составные объекты размером более (МБ)**

Исключение из проверки объектов больше указанного размера.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

Если флажок снят, Kaspersky Security для Windows Server проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстроедействие**.

- **Использовать технологию iSwift**

iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Security для Windows Server проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

По умолчанию флажок установлен.

- **Использовать технологию iChecker**

iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

Если флажок установлен, Kaspersky Security для Windows Server проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Security для Windows Server проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка иерархического хранилища

► Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Параметры области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. [542](#)).
2. Выберите закладку **Иерархическое хранилище**.
3. Выберите одно из следующих действий над файлами:

- **Не проверять**
- **Проверять только резидентную часть файла**
- **Проверять весь файл**

Если выбрано это действие, доступны следующие параметры проверки:

- Снимите или установите флажок **Только если зарегистрированы обращения к файлу за указанный период (дней)** и укажите количество дней.
- Снимите или установите флажок **По возможности не копировать файл на локальный жесткий диск**.

4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Проверка съемных дисков

► Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security** и выберите пункт **Настройка параметров проверки съемных дисков**.

Откроется окно **Проверка съемных дисков**.

2. В блоке **Проверка при подключении** выполните следующие действия:

- Установите флажок **Проверять съемные диски при подключении по USB**, если вы хотите, чтобы программа Kaspersky Security для Windows Server автоматически выполняла проверку съемных дисков при их подключении.
- Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
- В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

3. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

## Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые программа Kaspersky Security для Windows Server обработала с момента запуска задачи.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Security для Windows Server в журналах выполнения задач" на стр. [251](#)).

► Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

В таблице ниже приведена информация об объектах, которые программа Kaspersky Security для Windows Server обработала с момента запуска задачи.

Table 83. Статистика задач проверки по требованию

| Поле                                               | Описание                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обнаружено</b>                                  | Количество объектов, которые обнаружила программа Kaspersky Security для Windows Server. Например, если программа Kaspersky Security для Windows Server обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.                                                                                                                   |
| <b>Зараженных и других обнаруживаемых объектов</b> | Количество объектов, которые программа Kaspersky Security для Windows Server признала зараженными, или количество обнаруженных объектов, которые не были исключены из области действия задач проверки по требованию и были определены как легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным. |
| <b>Возможно зараженных объектов</b>                | Количество объектов, которые программа Kaspersky Security для Windows Server признала возможно зараженными.                                                                                                                                                                                                                                                             |

| Поле                                                 | Описание                                                                                                                                                                                                                                                       |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Объектов не вылечено</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server не вылечила по следующим причинам: <ul style="list-style-type: none"> <li>• Тип обнаруженного объекта не предполагает лечения.</li> <li>• При лечении возникла ошибка.</li> </ul> |
| <b>Объектов не помещено на карантин</b>              | Количество объектов, которые программе Kaspersky Security для Windows Server не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.                                                                                           |
| <b>Объектов не удалено</b>                           | Количество объектов, которые программе Kaspersky Security для Windows Server не удалось удалить, например, если доступ к объекту был заблокирован другой программой.                                                                                           |
| <b>Объектов не проверено</b>                         | Количество объектов в области защиты, которые программе Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.                                                                        |
| <b>Объектов, не помещенных в резервное хранилище</b> | Количество объектов, копии которых программе Kaspersky Security для Windows Server не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске.                                                                           |
| <b>Ошибок обработки</b>                              | Количество объектов, во время обработки которых возникла ошибка задачи.                                                                                                                                                                                        |
| <b>Вылечено объектов</b>                             | Количество объектов, которые вылечила программа Kaspersky Security для Windows Server.                                                                                                                                                                         |
| <b>Помещено на карантин</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server поместила на карантин.                                                                                                                                                            |
| <b>Помещено в резервное хранилище</b>                | Количество объектов, копии которых программа Kaspersky Security для Windows Server сохранила в резервном хранилище.                                                                                                                                            |
| <b>Удалено объектов</b>                              | Количество объектов, которые удалила программа Kaspersky Security для Windows Server.                                                                                                                                                                          |
| <b>Защищенных паролем объектов</b>                   | Количество объектов (например, архивов), которые программа Kaspersky Security для Windows Server пропустила, так как эти объекты защищены паролем.                                                                                                             |
| <b>Поврежденных объектов</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server пропустила, так как их формат искажен.                                                                                                                                            |
| <b>Обработано объектов</b>                           | Общее количество объектов, которые обработала программа Kaspersky Security для Windows Server.                                                                                                                                                                 |

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

## Создание и настройка задачи Мониторинг целостности файлов на основе эталона

► Чтобы создать или настроить задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Диагностика системы**.
2. Выберите пункт **Создать задачу Мониторинг целостности файлов на основе эталона**.  
Откроется окно **Добавить задачу**.
3. В раскрывающемся списке **Алгоритм расчета хеша** выберите один из следующих вариантов:
  - **MD5**
  - **SHA256**
4. В таблице **Области мониторинга** выполните следующие действия:
  - a. Чтобы добавить файл или папку в область задачи Мониторинг целостности файлов на основе эталона:
    1. Нажмите на кнопку **Добавить**.  
Откроется окно **Параметры области мониторинга**.
    2. Установите или снимите флажок **Контролировать эту область**.
    3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
    4. Установите флажок **Контролировать вложенные папки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.
    5. Нажмите на кнопку **ОК**.
  - b. Чтобы поменять файл или папку, добавленную ранее в область задачи Мониторинг целостности файлов на основе эталона:
    1. Нажмите на кнопку **Изменить**.  
Откроется окно **Параметры области мониторинга**.
    2. Установите или снимите флажок **Контролировать эту область**.
    3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
    4. Установите или снимите флажок **Контролировать вложенные папки**, чтобы включить или исключить все вложенные папки из области задачи Мониторинг целостности файлов на основе эталона.
    5. Нажмите на кнопку **ОК**.
  - c. Чтобы удалить файл или папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите этот файл или папку в таблице **Области мониторинга** и нажмите на кнопку **Удалить**.
5. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. [162](#)) на закладках **Расписание** и **Дополнительно**.
6. На закладке **Запуск с правами** настройте запуск задачи с правами определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. [165](#)).



7. В окне **Добавить задачу** нажмите на кнопку **ОК**.

Будет создана пользовательская задача Мониторинг целостности файлов на основе эталона. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (стр. [247](#)).

- *Чтобы просмотреть параметры задачи Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

## Управление задачами проверки по требованию с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина для защищаемых устройств в сети.

### Переход к мастеру создания задачи проверки по требованию

- *Чтобы создать локальную задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
5. Нажмите на кнопку **Добавить**.

Откроется окно **Мастер создания задачи**.

6. В раскрывающемся списке **Программы** выберите **Kaspersky Security для Windows Server**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. [523](#)).

- *Чтобы создать групповую задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.



3. Нажмите на кнопку **Добавить**.

Откроется окно **Мастер создания задачи**.

4. В раскрывающемся списке **Программы** выберите **Kaspersky Security для Windows Server**.
5. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
6. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. [523](#)).

- *Чтобы создать задачу проверки по требованию для произвольной группы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
2. Выберите выборку устройств, для которой требуется создать задачу.
3. Нажмите на кнопку **Запустить**.
4. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.
5. Нажмите на кнопку **Создать задачу**.
6. В раскрывающемся списке **Программы** выберите **Kaspersky Security для Windows Server**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. [523](#)).

- *Чтобы настроить задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
  2. Щелкните по названию задачи в списке задач Kaspersky Security Center.
- Откроется окно **<Название задачи>**.

## Переход к свойствам задачи проверки по требованию

- *Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
5. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
6. Перейдите на закладку **Параметры программы**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. [523](#)).

# Доверенная зона

Этот раздел содержит информацию о доверенной зоне Kaspersky Security для Windows Server, а также инструкции по добавлению объектов в доверенную зону при выполнении задач.

## В этом разделе

|                                                                |                     |
|----------------------------------------------------------------|---------------------|
| О доверенной зоне .....                                        | <a href="#">562</a> |
| Управление доверенной зоной с помощью Плагина управления ..... | <a href="#">564</a> |
| Управление доверенной зоной с помощью Консоли программы .....  | <a href="#">570</a> |
| Управление доверенной зоной с помощью Веб-плагина.....         | <a href="#">576</a> |

## О доверенной зоне

Доверенная зона – это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах Постоянная защита файлов, Защита трафика, Проверка скриптов и Защита RPC-подключаемых сетевых хранилищ, а также в задачах проверки по требованию.

Если при установке Kaspersky Security для Windows Server вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**, Kaspersky Security для Windows Server добавляет файлы, рекомендованные Microsoft и "Лабораторией Касперского", в доверенную зону для задач постоянной защиты компьютера.

Вы можете формировать доверенную зону Kaspersky Security для Windows Server по следующим правилам:

- **Доверенные процессы.** В доверенную зону помещаются объекты, чувствительные к перехватам файловых операций процессами программы.
- **Операции резервного копирования.** В доверенную зону помещаются объекты, доступ к которым выполняется при операциях резервного копирования жестких дисков на внешние устройства.
- **Исключения.** В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задачах Постоянная защита файлов, Защита трафика, Проверка скриптов, Защита RPC-подключаемых сетевых хранилищ, в пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный XML-файл, чтобы затем импортировать его в Kaspersky Security для Windows Server на другом защищаемом устройстве.

### Доверенные процессы

Применяется в задачах Постоянная защита файлов и Защита трафика.

Некоторые программы на защищаемом устройстве могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Security для Windows Server. К таким программам относятся, например, системные программы домен-контроллеров.

Чтобы не нарушать работу таких программ, вы можете выключить защиту файлов, к которым обращаются выполняющиеся процессы этих программ, сформировав в доверенной зоне список доверенных процессов.

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Имена некоторых из них приведены на веб-сайте Microsoft <https://www.microsoft.com/ru-ru/> (код статьи: KB822158).

Вы можете включать и выключать применение доверенных процессов в доверенной зоне.

Если исполняемый файл изменяется, например, в результате обновления, Kaspersky Security для Windows Server исключает его из списка доверенных процессов.

Программа не использует путь к файлу на защищаемом устройстве для идентификации процесса как доверенного. Путь к файлу на защищаемом устройстве применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

## Операции резервного копирования

Применяется в задачах постоянной защиты сервера.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства можно выключить защиту объектов, доступ к которым осуществляется при операциях резервного копирования. Kaspersky Security для Windows Server будет проверять объекты, которые программа резервного копирования открывает на чтение с признаком FILE\_FLAG\_BACKUP\_SEMANTICS.

## Исключения

Применяются в задачах Постоянная защита файлов, Защита трафика, Защита RPC-подключаемых сетевых хранилищ и в задачах проверки по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в параметрах уровня безопасности каждой задачи Kaspersky Security для Windows Server по отдельности.

Вы можете добавлять в доверенную зону исключения по их расположению на защищаемом устройстве, по имени или маске имени обнаруженного объекта или использовать оба параметра.

На основании исключения Kaspersky Security для Windows Server может пропускать в указанных задачах объекты согласно следующим параметрам:

- указанные объекты, обнаруживаемые по имени или маске имени в указанных областях защищаемого устройства или сетевого хранилища;
- все объекты, обнаруживаемые в указанных областях защищаемого устройства или сетевого хранилища;
- указанные объекты, обнаруживаемые по имени или маске имени во всей области защиты или проверки.

## Управление доверенной зоной с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка доверенной зоны для одного или всех защищаемых устройств в сети.

### В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| Навигация .....                                                         | <a href="#">564</a> |
| Настройка параметров доверенной зоны с помощью Плагина управления ..... | <a href="#">565</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                         |                     |
|---------------------------------------------------------|---------------------|
| Переход к параметрам политики для доверенной зоны ..... | <a href="#">564</a> |
| Переход к окну параметров доверенной зоны .....         | <a href="#">565</a> |

## Переход к параметрам политики для доверенной зоны

► Чтобы перейти к доверенной зоне в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительно**.
6. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

## Переход к окну параметров доверенной зоны

► Чтобы настроить доверенную зону в окне свойств программы, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
  - двойным щелчком мыши на имени защищаемого устройства;
  - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. В разделе **Программы** выберите **Kaspersky Security для Windows Server**.
6. Нажмите на кнопку **Свойства**.

Откроется окно **Параметры программы Kaspersky Security для Windows Server**.

7. Выберите раздел **Дополнительные возможности**.
8. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

## Настройка параметров доверенной зоны с помощью Плагина управления

По умолчанию доверенная зона применяется ко всем новым политикам и задачам.

► Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Security для Windows Server пропускает при выполнении задачи (см. раздел "Добавление исключений" на стр. [566](#)).
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Security для Windows Server пропускает при выполнении задачи (см. раздел "Добавление доверенных процессов" на стр. [567](#)).
3. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. [569](#)).

### В этом разделе

|                                       |                     |
|---------------------------------------|---------------------|
| Добавление исключений .....           | <a href="#">566</a> |
| Добавление доверенных процессов ..... | <a href="#">567</a> |
| Использование маски not-a-virus ..... | <a href="#">569</a> |

## Добавление исключений

- Чтобы добавить исключение в доверенную зону в политике Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Доверенная зона** (см. раздел "Переход к параметрам политики доверенной зоны" на стр. [564](#)).
2. На закладке **Исключения** укажите объекты, которые Kaspersky Security для Windows Server пропускает при проверке:

- Чтобы создать рекомендуемые исключения, нажмите на кнопку **Добавить рекомендуемые исключения**.

При нажатии на эту кнопку в список исключений добавляются исключения, рекомендованные корпорацией Microsoft и "Лабораторией Касперского".

- Чтобы импортировать исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файлы, которые Kaspersky Security для Windows Server будет считать доверенными.
- Чтобы вручную указать условия, при выполнении которых файл будет считаться доверенным, нажмите на кнопку **Добавить**.

Откроется окно **Исключения**.

3. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

- Чтобы исключить объект из области защиты или проверки:

- a. Установите флажок **Проверяемый объект**.

Добавляет файл, папку, диск или файл скрипта в исключения.

Если флажок установлен, Kaspersky Security для Windows Server пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Security для Windows Server, выбранных в разделе **Область применения правил**.

По умолчанию флажок снят.

- b. Нажмите на кнопку **Изменить**.

Откроется окно **Выбор объекта**.

- c. Выберите объект, который вы хотите исключить из области проверки.

При указании объектов можно использовать маски имени (с помощью символов ? и \*) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Security для Windows Server при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Security для Windows Server обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

- d. Нажмите на кнопку **ОК**.

- e. Установите флажок **Применить к вложенным папкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Чтобы указать имя обнаруживаемого объекта:

a. Установите флажок **Обнаруживаемые объекты**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

b. Нажмите на кнопку **Изменить**.

Откроется окно **Список обнаруживаемых объектов**.

c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

d. Нажмите на кнопку **Добавить**.

e. Нажмите на кнопку **ОК**.

4. В разделе **Область применения исключений** установите флажки рядом с названиями задач, к которым вы хотите применить исключения.

Название задачи Kaspersky Security для Windows Server, в которой применяется правило.

5. Нажмите на кнопку **ОК**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

## Добавление доверенных процессов

► Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:

1. Откройте окно **Доверенная зона** (см. раздел "Переход к параметрам политики доверенной зоны" на стр. 564).

2. Выберите закладку **Доверенные процессы**.

3. Установите флажок **Не проверять операции резервного копирования файлов**, чтобы пропустить проверку операций чтения файлов.

Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом устройстве.

Если флажок установлен, Kaspersky Security для Windows Server пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

Если флажок снят, Kaspersky Security для Windows Server проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

По умолчанию флажок установлен.

4. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

Флажок включает или выключает проверку файловой активности доверенных процессов.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server проверяет файловые операции доверенных процессов.

По умолчанию флажок снят.

5. Нажмите на кнопку **Добавить**.
6. В контекстном меню кнопки выберите один из следующих вариантов:

- **Несколько процессов**

В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

- a. **Использовать полный путь для определения доверенности процесса**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

- b. **Использовать хеш файла для определения доверенности процесса**

Если флажок установлен, Kaspersky Security для Windows Server использует хеш выбранного файла для определения, является ли процесс доверенным.

Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

По умолчанию флажок установлен.

- c. Чтобы добавить данные на основе исполняемых процессов, нажмите на кнопку **Обзор**.

- d. Выберите исполняемый файл в открывшемся окне.

Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

- e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

- f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

- g. Нажмите на кнопку **ОК**.

Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Security для Windows Server, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.



- **Один процесс на основе имени файла и пути**

В открывшемся окне **Добавление процесса** выполните следующие действия:

- а. Укажите путь к исполняемому файлу (включая имя файла).

При указании объектов можно использовать маски имени (с помощью символов ? и \*) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Security для Windows Server при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Security для Windows Server обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

- б. Нажмите на кнопку **ОК**.

- **Один процесс на основе свойств объекта**

В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

- а. Нажмите на кнопку **Обзор** и выберите процесс.

- б. **Использовать полный путь для определения доверенности процесса**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

- в. **Использовать хеш файла для определения доверенности процесса**

Если флажок установлен, Kaspersky Security для Windows Server использует хеш выбранного файла для определения, является ли процесс доверенным.

Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

По умолчанию флажок установлен.

- д. Нажмите на кнопку **ОК**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

7. В окне **Доверенная зона** нажмите на кнопку **ОК**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

## Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.
- Проверка скриптов.

- Защита RPC-подключаемых сетевых хранилищ.
- Защита трафика.

Если маска не добавлена в список исключений, Kaspersky Security для Windows Server выполнит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел "Переход к параметрам политики доверенной зоны" на стр. [564](#)).
2. На закладке **Исключения** в графе **Обнаруживаемые объекты** прокрутите список и выберите строку со значением *not-a-virus:\**, если флажок снят.
3. Нажмите на кнопку **ОК**.

Новые параметры будут применены.

## Управление доверенной зоной с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка доверенной зоны для защищаемого устройства.

### В этом разделе

|                                                                  |                     |
|------------------------------------------------------------------|---------------------|
| Использование доверенной зоны для задач в Консоли программы..... | <a href="#">570</a> |
| Настройка параметров доверенной зоны в Консоли программы.....    | <a href="#">571</a> |

## Использование доверенной зоны для задач в Консоли программы

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

После того как вы включите или выключите доверенную зону, заданные в ней исключения начнут или перестанут действовать в выполняющихся задачах немедленно.

► *Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Security для Windows Server, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить использование доверенной зоны.
2. Выберите пункт **Свойства**.  
Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** выполните одно из следующих действий:

- Чтобы применить доверенную зону в задаче, установите флажок **Применить доверенную зону**.
  - Чтобы выключить применение доверенной зоны в задаче, снимите флажок **Применить доверенную зону**.
4. Чтобы настроить параметры доверенной зоны, перейдите по ссылке в названии флажка **Применить доверенную зону**.
- Откроется окно **Доверенная зона**.
- В окне **Доверенная зона** настройте исключения (см. раздел "Добавление исключений в доверенную зону" на стр. [571](#)) и доверенные процессы (см. раздел "Добавление доверенных процессов" на стр. [573](#)) и нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в окне **Параметры задачи**, чтобы сохранить изменения.

## Настройка параметров доверенной зоны в Консоли программы

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Security для Windows Server пропускает при выполнении задачи (см. раздел "Добавление исключений в доверенную зону" на стр. [571](#)).
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Security для Windows Server пропускает при выполнении задачи (см. раздел "Добавление доверенных процессов" на стр. [573](#)).
3. Примените доверенную зону для задач программы (см. раздел "Использование доверенной зоны для задач в Консоли программы" на стр. [570](#)).
4. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. [575](#)).

### В этом разделе

|                                               |                     |
|-----------------------------------------------|---------------------|
| Добавление исключений в доверенную зону ..... | <a href="#">571</a> |
| Добавление доверенных процессов .....         | <a href="#">573</a> |
| Использование маски not-a-virus .....         | <a href="#">575</a> |

## Добавление исключений в доверенную зону

- Чтобы вручную добавить исключение в доверенную зону в Консоли программы, выполните следующие действия:
1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
  2. Выберите в меню пункт **Настроить параметры доверенной зоны**.
- Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
  4. Нажмите на кнопку **Добавить**.
- Откроется окно **Исключения**.

5. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

- Чтобы исключить объект из области защиты или проверки:

- а. Установите флажок **Проверяемый объект**.

Добавляет файл, папку, диск или файл скрипта в исключения.

Если флажок установлен, Kaspersky Security для Windows Server пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Security для Windows Server, выбранных в разделе **Область применения правил**.

По умолчанию флажок снят.

- б. Нажмите на кнопку **Изменить**.

Откроется окно **Выбор объекта**.

- в. Выберите объект, который вы хотите исключить из области проверки.

При указании объектов можно использовать маски имени (с помощью символов ? и \*) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Security для Windows Server при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Security для Windows Server обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

- г. Нажмите на кнопку **ОК**.

- е. Установите флажок **Применить к вложенным папкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Чтобы указать имя обнаруживаемого объекта:

- а. Установите флажок **Обнаруживаемые объекты**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- б. Нажмите на кнопку **Изменить**.

Откроется окно **Список обнаруживаемых объектов**.

- в. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

- г. Нажмите на кнопку **Добавить**.

- е. Нажмите на кнопку **ОК**.

6. В разделе **Область применения исключений** установите флажки рядом с названиями задач, к которым вы хотите применить исключения.

Название задачи Kaspersky Security для Windows Server, в которой применяется правило.

7. Нажмите на кнопку **ОК**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

## Добавление доверенных процессов

Вы можете добавить процесс в список доверенных процессов одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом устройстве;
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

Если исполняемый файл процесса изменится, Kaspersky Security для Windows Server исключит этот процесс из списка доверенных процессов.

- Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.  
Откроется окно **Доверенная зона**.
3. Выберите закладку **Доверенные процессы**.
4. Установите флажок **Не проверять операции резервного копирования файлов**, чтобы пропустить проверку операций чтения файлов.

Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом устройстве.

Если флажок установлен, Kaspersky Security для Windows Server пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

Если флажок снят, Kaspersky Security для Windows Server проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

По умолчанию флажок установлен.

5. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

Флажок включает или выключает проверку файловой активности доверенных процессов.

Если флажок установлен, Kaspersky Security для Windows Server пропускает при проверке операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server проверяет файловые

операции доверенных процессов.

По умолчанию флажок снят.

6. Нажмите на кнопку **Добавить**.

7. В контекстном меню кнопки выберите один из следующих вариантов:

- **Несколько процессов**

В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

a. **Использовать полный путь для определения доверенности процесса**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

b. **Использовать хеш файла для определения доверенности процесса**

Если флажок установлен, Kaspersky Security для Windows Server использует хеш выбранного файла для определения, является ли процесс доверенным.

Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

По умолчанию флажок установлен.

c. Чтобы добавить данные на основе исполняемых процессов, нажмите на кнопку **Обзор**.

d. Выберите исполняемый файл в открывшемся окне.

Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

g. Нажмите на кнопку **ОК**.

Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Security для Windows Server, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

- **Один процесс на основе имени файла и пути**

В открывшемся окне **Добавление процесса** выполните следующие действия:

a. Укажите путь к исполняемому файлу (включая имя файла).

При указании объектов можно использовать маски имени (с помощью символов ? и \*) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Security для Windows Server при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Security для Windows Server обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

b. Нажмите на кнопку **ОК**.

- **Один процесс на основе свойств объекта**

В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

a. Нажмите на кнопку **Обзор** и выберите процесс.

b. **Использовать полный путь для определения доверенности процесса**

Если выбран этот вариант, Kaspersky Security для Windows Server использует полный путь к файлу для определения, является ли процесс доверенным.

c. **Использовать хеш файла для определения доверенности процесса**

Если флажок установлен, Kaspersky Security для Windows Server использует хеш выбранного файла для определения, является ли процесс доверенным.

Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

По умолчанию флажок установлен.

d. Нажмите на кнопку **ОК**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

8. В окне **Доверенная зона** нажмите на кнопку **ОК**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

## Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.
- Проверка скриптов.
- Защита RPC-подключаемых сетевых хранилищ.
- Защита трафика.

Если маска не добавлена в список исключений, Kaspersky Security для Windows Server выполнит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

► Чтобы использовать маску *not-a-virus*, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.  
Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Прокрутите список до элемента *not-a-virus*:\*.
5. Установите соответствующий флажок, если он снят.
6. Нажмите на кнопку **ОК**.

Новые параметры будут применены.

## Управление доверенной зоной с помощью Веб-плагина

Чтобы настроить доверенную зону с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.
6. Настройте доверенную зону в соответствии с вашими требованиями (см. раздел "Настройка параметров доверенной зоны с помощью Плагина управления" на стр. [565](#)).



# Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

## В этом разделе

|                                                                     |                     |
|---------------------------------------------------------------------|---------------------|
| О защите от эксплойтов .....                                        | <a href="#">577</a> |
| Управление защитой от эксплойтов с помощью Плагина управления ..... | <a href="#">578</a> |
| Управление защитой от эксплойтов с помощью Консоли программы .....  | <a href="#">582</a> |
| Управление защитой от эксплойтов с помощью Веб-плагина .....        | <a href="#">586</a> |
| Техники защиты от эксплойтов .....                                  | <a href="#">589</a> |

## О защите от эксплойтов

Kaspersky Security для Windows Server предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее "Агент") в защищаемый процесс.

Агент защиты процессов – это динамически загружаемый модуль Kaspersky Security для Windows Server, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

**Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, вам нужно завершить данный процесс. Может потребоваться перезагрузка защищаемого устройства (например, при защите системного процесса).**

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Security для Windows Server выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;

- удалить процесс из списка защищаемых и перезапустить его.

## Служба Kaspersky Security Exploit Prevention

Для максимальной эффективности компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Exploit Prevention на защищаемом устройстве. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемое устройство создается и запускается процесс kavfswd. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

После остановки службы Kaspersky Security Exploit Prevention программа продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники защиты от эксплойтов для защиты памяти процессов.

Если на устройстве установлена операционная система Windows 10 или более поздних версий, программа не будет продолжать защищать процессы и память процессов после остановки службы Kaspersky Security Exploit Prevention.

В случае остановки службы Kaspersky Security Exploit Prevention программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе данные об атаках эксплойтов и о завершении процессов). Также Агент не сможет получать данные о новых параметрах защиты и о добавлении новых процессов в список защищаемых процессов.

## Режимы защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из следующих режимов:

- **Завершать скомпрометированные процессы:** применяйте данный режим, чтобы завершать процесс при попытке эксплуатации уязвимости.

При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Security для Windows Server не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Только сообщать:** применяйте этот режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале безопасности.

В этом режиме Kaspersky Security для Windows Server регистрирует все попытки эксплуатации уязвимостей посредством создания событий.

## Управление защитой от эксплойтов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров компонента для защищаемых устройств в сети.

## В этом разделе

|                                            |                     |
|--------------------------------------------|---------------------|
| Навигация .....                            | <a href="#">579</a> |
| Настройка защиты памяти процессов .....    | <a href="#">580</a> |
| Добавление процесса в область защиты ..... | <a href="#">581</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

## В этом разделе

|                                                              |                     |
|--------------------------------------------------------------|---------------------|
| Переход к параметрам политики для защиты от эксплойтов ..... | <a href="#">579</a> |
| Переход к окну параметров защиты от эксплойтов .....         | <a href="#">579</a> |

## Переход к параметрам политики для защиты от эксплойтов

- *Чтобы перейти к параметрам защиты от эксплойтов в политике Kaspersky Security Center, выполните следующие действия:*
  1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой вы хотите настроить задачу.
  3. Выберите закладку **Политики**.
  4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
  5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита сервера**.
  6. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.  
Откроется окно **Защита от эксплойтов**.  
Настройте защиту от эксплойтов в соответствии с вашими требованиями.

## Переход к окну параметров защиты от эксплойтов

- *Чтобы перейти к окну свойства для защиты от эксплойтов, выполните следующие действия:*
  1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой вы хотите настроить задачу.

3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
  - двойным щелчком мыши на имени защищаемого устройства;
  - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.
 Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Security для Windows Server**.
6. Нажмите на кнопку **Свойства**.  
Откроется окно **Параметры программы Kaspersky Security для Windows Server**.
7. Перейдите в раздел **Постоянная защита сервера**.
8. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.  
Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

## Настройка защиты памяти процессов

► Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. [579](#)).
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
  - **Защищать процессы от эксплуатации уязвимостей**  
 Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.  
  
 Если флажок снят, Kaspersky Security для Windows Server не защищает процессы устройства от эксплуатации уязвимостей.  
  
 По умолчанию флажок снят.
  - **Завершать скомпрометированные процессы**  
 Если выбран данный режим, Kaspersky Security для Windows Server завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.
  - **Только сообщать**  
 Если выбран данный режим, Kaspersky Security для Windows Server сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.  
  
 Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Security для Windows Server обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только сообщать**.
3. В разделе **Профилактические действия** настройте следующие параметры:

- **Сообщать о скомпрометированных процессах посредством службы терминалов**

Если флажок установлен, Kaspersky Security для Windows Server отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

Если флажок снят, Kaspersky Security для Windows Server не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

- **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**

Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Security для Windows Server не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

Если флажок снят, Kaspersky Security для Windows Server не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

По умолчанию флажок установлен.

#### 4. В окне **Защита от эксплойтов** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Можно исключить процессы из области защиты, сняв соответствующие флажки в списке процессов.

### ► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. [579](#)).
2. На закладке **Защищаемые процессы** нажмите на кнопку **Обзор**.  
Откроется окно проводника Windows.
3. Выберите процесс, который вы хотите добавить в список.
4. Нажмите на кнопку **Открыть**.  
Имя процесса будет отображено в строке.
5. Нажмите на кнопку **Добавить**.  
Указанный процесс добавится в список защищаемых процессов.
6. Выберите добавленный процесс.
7. Нажмите на кнопку **Указать техники защиты от эксплойтов**.

Откроется окно **Техники защиты от эксплойтов**.

8. Выберите один из следующих вариантов применения техник снижения рисков:

- **Применять все доступные техники защиты от эксплойтов**

Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

- **Применять выбранные техники защиты от эксплойтов**

Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

а. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

б. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

9. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

- Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей**.

- В поле **Не запрещать модули, если они запущены в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:

- Интернет
- Интранет
- Доверенные веб-сайты
- Сайты с ограниченным доступом
- Компьютер

Данные параметры применимы только для Internet Explorer®.

10. Нажмите на кнопку **ОК**.

Процесс будет добавлен в область защиты задачи.

## Управление защитой от эксплойтов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров компонента на защищаемом устройстве.

### В этом разделе

|                                            |                     |
|--------------------------------------------|---------------------|
| Навигация .....                            | <a href="#">583</a> |
| Настройка защиты памяти процессов .....    | <a href="#">583</a> |
| Добавление процесса в область защиты ..... | <a href="#">584</a> |

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

### В этом разделе

|                                                                      |                     |
|----------------------------------------------------------------------|---------------------|
| Переход к основным параметрам защиты от эксплойтов .....             | <a href="#">583</a> |
| Переход к параметрам защиты процессов при защите от эксплойтов ..... | <a href="#">583</a> |

### Переход к основным параметрам защиты от эксплойтов

- Чтобы перейти к окну **Параметры защиты от эксплойтов**, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Security**.
2. В контекстном меню выберите пункт **Защита от эксплойтов: общие параметры**.

Откроется окно **Параметры защиты от эксплойтов**.

Настройте общие параметры защиты от эксплойтов в соответствии с вашими требованиями.

### Переход к параметрам защиты процессов при защите от эксплойтов

- Чтобы перейти к окну **Параметры защиты процессов**, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Security**.
2. В контекстном меню выберите пункт **Защита от эксплойтов: параметры защиты процессов**.

Откроется окно **Параметры защиты процессов**.

Настройте параметры защиты процессов для защиты от эксплойтов в соответствии с вашими требованиями.

## Настройка защиты памяти процессов

- Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:

1. Откройте окно **Параметры защиты от эксплойтов**.
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:

- **Защищать процессы от эксплуатации уязвимостей**

Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

Если флажок снят, Kaspersky Security для Windows Server не защищает процессы устройства от эксплуатации уязвимостей.

По умолчанию флажок снят.

- **Завершать скомпрометированные процессы**

Если выбран данный режим, Kaspersky Security для Windows Server завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

- **Только сообщать**

Если выбран данный режим, Kaspersky Security для Windows Server сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.

Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Security для Windows Server обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только сообщать**.

3. В разделе **Профилактические действия** настройте следующие параметры:

- **Сообщать о скомпрометированных процессах посредством службы терминалов**

Если флажок установлен, Kaspersky Security для Windows Server отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

Если флажок снят, Kaspersky Security для Windows Server не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

- **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**

Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Security для Windows Server не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

Если флажок снят, Kaspersky Security для Windows Server не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

По умолчанию флажок установлен.

4. В окне **Параметры защиты от эксплойтов** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Вы можете исключить какой-либо процесс из защиты, сняв флажок в соответствующей строке процесса.



► Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:

1. Откройте окно **Параметры защиты процесса**.
2. Чтобы защитить процесс от компрометации и снизить возможное влияние эксплуатации уязвимостей, выполните следующие действия:
  - a. Нажмите на кнопку **Обзор**.  
Откроется стандартное окно Microsoft Windows **Открыть**.
  - b. В открывшемся окне выберите процесс, который вы хотите добавить в список.
  - c. Нажмите на кнопку **Открыть**.
  - d. Нажмите на кнопку **Добавить**.  
Указанный процесс добавится в список защищаемых процессов.
3. Выберите добавленный процесс в списке.
4. Текущая конфигурация отображается на закладке **Параметры защиты процессов**:
  - **Имя процесса**
  - **Выполняется сейчас**
  - **Применяемые техники защиты от эксплойтов**
  - **Техника Attack Surface Reduction**
5. Чтобы изменить применяемые к процессу техники защиты от эксплойтов, выберите закладку **Техники защиты от эксплойтов**.
6. Выберите один из следующих вариантов применения техник снижения рисков:
  - **Применять все доступные техники защиты от эксплойтов**  
Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
  - **Применять указанные техники защиты от эксплойтов**  
Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.
    - a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
7. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
  - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей**.
  - В разделе **Не запрещать модули, если они запущены в зоне интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
    - **Интернет**
    - **Инtranет**
    - **Доверенные веб-сайты**
    - **Сайты с ограниченным доступом**
    - **Компьютер**

Данные параметры применимы только для Internet Explorer®.

8. Нажмите на кнопку **Сохранить**.

Процесс будет добавлен в область защиты задачи.

## Управление защитой от эксплойтов с помощью Веб-плаги́на

В этом разделе описана навигация в интерфейсе Веб-плаги́на и настройка параметров компонента на защищаемом устройстве.

### В этом разделе

|                                            |                     |
|--------------------------------------------|---------------------|
| Настройка защиты памяти процессов .....    | <a href="#">586</a> |
| Добавление процесса в область защиты ..... | <a href="#">587</a> |

## Настройка защиты памяти процессов

- Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.
6. Откройте закладку **Параметры защиты от эксплойтов**.
7. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:

- **Защищать процессы от эксплуатации уязвимостей**

Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

Если флажок снят, Kaspersky Security для Windows Server не защищает процессы устройства от эксплуатации уязвимостей.

По умолчанию флажок снят.

- **Завершать скомпрометированные процессы**

Если выбран данный режим, Kaspersky Security для Windows Server завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

- **Только сообщать**

Если выбран данный режим, Kaspersky Security для Windows Server сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.

Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Security для Windows Server обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только сообщать**.

8. В разделе **Профилактические действия** настройте следующие параметры:

- **Сообщать о скомпрометированных процессах посредством службы терминалов**

Если флажок установлен, Kaspersky Security для Windows Server отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

Если флажок снят, Kaspersky Security для Windows Server не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

- **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**

Если флажок установлен, Kaspersky Security для Windows Server снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Security для Windows Server не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

Если флажок снят, Kaspersky Security для Windows Server не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

По умолчанию флажок установлен.

9. В окне **Защита от эксплойтов** нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.
6. Перейдите на закладку **Защищенные процессы**.

7. Нажмите на кнопку **Добавить**.
8. Откроется окно **Техники защиты от эксплойтов**.
9. Укажите название процесса.
10. Выберите один из следующих вариантов применения техник снижения рисков:

- **Применять все доступные техники защиты от эксплойтов**

Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

- **Применять выбранные техники защиты от эксплойтов**

Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

11. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

- Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей**.
- В поле **Не запрещать модули, если они запущены в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:

- **Интернет**
- **Инtranет**
- **Доверенные веб-сайты**
- **Сайты с ограниченным доступом**
- **Компьютер**

Данные параметры применимы только для Internet Explorer®.

12. Нажмите на кнопку **ОК**.

Процесс будет добавлен в область защиты задачи.

## Техники защиты от эксплойтов

Table 84. Техники защиты от эксплойтов

| Техника защиты от эксплойтов                                                                            | Описание                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Execution Prevention (DEP)                                                                         | Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.                                               |
| Address Space Layout Randomization (ASLR)                                                               | Изменение расположения структур данных в адресном пространстве процесса.                                                                           |
| Structured Exception Handler Overwrite Protection (SEHOP)                                               | Подмена записи в структуре исключений или подмена обработчика исключений.                                                                          |
| Null Page Allocation                                                                                    | Предотвращение переориентации нулевого указателя.                                                                                                  |
| LoadLibrary Network Call Check (Anti ROP)                                                               | Защита от загрузки динамических библиотек с сетевых путей.                                                                                         |
| Executable Stack (Anti ROP)                                                                             | Запрет на несанкционированное исполнение областей стека.                                                                                           |
| Anti RET Check (Anti ROP)                                                                               | Проверка безопасного вызова функции через CALL инструкцию.                                                                                         |
| Anti Stack Pivoting (Anti ROP)                                                                          | Защита от перемещения указателя стека ESP на эксплуатируемый адрес.                                                                                |
| Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register) | Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll.                      |
| Heap Spray Allocation (Heapspray)                                                                       | Защита от выделения памяти под исполнение вредоносного кода.                                                                                       |
| Execution Flow Simulation (Anti Return Oriented Programming)                                            | Обнаружение потенциально опасных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.                                               |
| IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))                           | Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile). |
| Attack Surface Reduction (ASR)                                                                          | Блокирование запуска уязвимых модулей через защищаемый процесс.                                                                                    |
| Anti Process Hollowing (Hollowing)                                                                      | Защита от создания и запуска вредоносных копий доверенных процессов.                                                                               |
| Anti AtomBombing (APC)                                                                                  | Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC).                                                          |
| Anti CreateLocalThread (RThreadRemote)                                                                  | Сторонний процесс создал поток в защищаемом процессе.                                                                                              |
| Anti CreateRemoteThread (RThreadRemote)                                                                 | Защита внедрения потока защищаемого процесса в другой процесс.                                                                                     |

# Управление иерархическим хранилищем

Этот раздел содержит информацию об антивирусной проверке файлов, расположенных в иерархических хранилищах и системах резервного копирования.

## В этом разделе

|                                                                    |                     |
|--------------------------------------------------------------------|---------------------|
| Об иерархическом хранилище .....                                   | <a href="#">590</a> |
| Настройка параметров HSM-системы с помощью Плагина управления..... | <a href="#">591</a> |
| Настройка параметров HSM-системы в Консоли программы .....         | <a href="#">592</a> |
| Настройка параметров HSM-системы с помощью Веб-плагина .....       | <a href="#">593</a> |

## Об иерархическом хранилище

Система управления иерархическим хранилищем (англ. Hierarchical Storage Management, далее также "HSM-система") позволяет перемещать данные между быстрыми локальными дисками и медленными устройствами долговременного хранения информации. Несмотря на очевидные преимущества быстрых запоминающих устройств, для большинства организаций их использование оказывается слишком дорогим. HSM-системы обеспечивают перенос неиспользуемой информации на недорогие устройства удаленного хранения, сокращая экономические издержки компании.

HSM-системы хранят часть данных в удаленных хранилищах и восстанавливают их в случае необходимости. При этом HSM-системы ведут постоянный мониторинг обращения к файлам, определяя, какие из них можно переместить в удаленное хранилище, а какие целесообразно хранить локально. Файлы перемещаются в удаленное хранилище, если к ним не поступает обращений за указанный период времени. Если пользователь обращается к файлу, расположенному в удаленном хранилище, этот файл переносится обратно на локальный диск. Этот принцип обеспечивает пользователям быстрый доступ к большим объемам данных, существенно превышающим размеры доступного пространства на локальном диске.

При перемещении файла с локального диска в удаленное хранилище HSM-система сохраняет ссылку на фактическое расположение файла. При обращении к такому файлу система определяет его местоположение на резервном устройстве. Замещение файлов ссылками на их местоположение в удаленном хранилище позволяет создавать хранилища данных практически неограниченного размера.

Некоторые HSM-системы позволяют сохранять части файлов в локальном хранилище. При этом большая часть файла перемещается в удаленное хранилище, а в локальном хранилище остается небольшая часть исходного файла.

В HSM-системах применяется следующие способы доступа к информации, помещенной в иерархическое хранилище:

- точки повторной обработки;
- расширенные атрибуты файла.

## Настройка параметров HSM-системы с помощью Плагина управления

Если вы не используете HSM-системы, не меняйте заданное по умолчанию значение параметра Тип доступа к иерархическому хранилищу (Не HSM-система).

Для настройки доступа к иерархическому хранилищу вам нужно указать, каким образом HSM-система определяет местоположение проверяемого файла. Вы можете найти эту информацию в документации к используемой HSM-системе.

► Чтобы задать тип доступа к иерархическому хранилищу, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. В подразделе **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.  
Откроется окно **Дополнительные параметры программы**.
7. Выберите закладку **Иерархическое хранилище**.
8. Выберите тип доступа к HSM-системе:

- **Не HSM-система**

Kaspersky Security для Windows Server не использует параметры HSM-системы при выполнении задач проверки по требованию.

Этот вариант выбран по умолчанию.

- **HSM-система использует точки повторной обработки**

Kaspersky Security для Windows Server использует точки повторной обработки для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

- **HSM-система использует расширенные атрибуты файлов**

Kaspersky Security для Windows Server использует расширенные атрибуты файла для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

- **Неизвестная HSM-система**

Kaspersky Security для Windows Server проверяет все файлы как файлы, расположенные в удаленном хранилище, при выполнении задач проверки по

требованию.

Не рекомендуется использовать этот вариант.

Если указана неверная версия или выбран вариант **Неизвестная HSM-система**, Kaspersky Security для Windows Server может неверно определять местоположение объектов, что увеличит время обработки объектов.

9. Нажмите на кнопку **ОК**.

Настроенные параметры HSM-системы будут сохранены.

## Настройка параметров HSM-системы с помощью Консоли программы

Если вы не используете HSM-системы, не меняйте заданное по умолчанию значение параметра Тип доступа к иерархическому хранилищу (Не HSM-система).

Для настройки доступа к иерархическому хранилищу вам нужно указать, каким образом HSM-система определяет местоположение проверяемого файла. Вы можете найти эту информацию в документации к используемой HSM-системе.

► Чтобы задать тип доступа к иерархическому хранилищу, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите пункт **Иерархическое хранилище**.

Откроется окно **Параметры HSM-системы**.

3. На закладке **Иерархическое хранилище** укажите параметры HSM-системы:

- **Не HSM-система**

Kaspersky Security для Windows Server не использует параметры HSM-системы при выполнении задач проверки по требованию.

Этот вариант выбран по умолчанию.

- **HSM-система использует точки повторной обработки**

Kaspersky Security для Windows Server использует точки повторной обработки для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

- **HSM-система использует расширенные атрибуты файлов**

Kaspersky Security для Windows Server использует расширенные атрибуты файла для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.



- **Неизвестная HSM-система**

Kaspersky Security для Windows Server проверяет все файлы как файлы, расположенные в удаленном хранилище, при выполнении задач проверки по требованию.

Не рекомендуется использовать этот вариант.

Если указана неверная версия или выбран вариант **Неизвестная HSM-система**, Kaspersky Security для Windows Server может неверно определять местоположение объектов, что увеличит время обработки объектов.

4. Нажмите на кнопку **ОК**.

Настроенные параметры HSM-системы будут сохранены.

## Настройка параметров HSM-системы с помощью Веб-плаги́на

Если вы не используете HSM-системы, не меняйте заданное по умолчанию значение параметра Тип доступа к иерархическому хранилищу (Не HSM-система).

Для настройки доступа к иерархическому хранилищу вам нужно указать, каким образом HSM-система определяет местоположение проверяемого файла. Вы можете найти эту информацию в документации к используемой HSM-системе.

► Чтобы задать тип доступа к иерархическому хранилищу, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. В подразделе **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.  
Откроется окно **Масштабируемость и интерфейс**.
6. В разделе **Параметры HSM-системы** выберите вариант доступа к HSM-системе:

- **Не HSM-система**

Kaspersky Security для Windows Server не использует параметры HSM-системы при выполнении задач проверки по требованию.

Этот вариант выбран по умолчанию.

- **HSM-система использует точки повторной обработки**

Kaspersky Security для Windows Server использует точки повторной обработки для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

- **HSM-система использует расширенные атрибуты файлов**

Kaspersky Security для Windows Server использует расширенные атрибуты файла для проверки файлов в удаленном хранилище при выполнении задач проверки по требованию.

- **Неизвестная HSM-система**

Kaspersky Security для Windows Server проверяет все файлы как файлы, расположенные в удаленном хранилище, при выполнении задач проверки по требованию.

Не рекомендуется использовать этот вариант.

Если указана неверная версия или выбран вариант **Неизвестная HSM-система**, Kaspersky Security для Windows Server может неверно определять местоположение объектов, что увеличит время обработки объектов.

7. Нажмите на кнопку **ОК**.

Настроенные параметры HSM-системы будут сохранены.

# Защита сетевых хранилищ

Этот раздел содержит информацию о сетевом хранилище и о настройке его параметров.

## В этом разделе

|                                                                                |                     |
|--------------------------------------------------------------------------------|---------------------|
| Интеграция Kaspersky Security для Windows Server с сетевыми хранилищами .....  | <a href="#">596</a> |
| Работа с Консолью Kaspersky Security для Windows Server .....                  | <a href="#">600</a> |
| Защита сетевых хранилищ EMC группы Celerra / VNX .....                         | <a href="#">611</a> |
| Защита RPC-подключаемых сетевых хранилищ .....                                 | <a href="#">613</a> |
| Защита ICAP-подключаемых сетевых хранилищ .....                                | <a href="#">634</a> |
| Защита от шифрования для NetApp .....                                          | <a href="#">647</a> |
| Управление задачами защиты сетевых хранилищ из Kaspersky Security Center ..... | <a href="#">660</a> |

## Интеграция Kaspersky Security для Windows Server с сетевыми хранилищами

В этом разделе приведена информация о принципах совместной работы Kaspersky Security для Windows Server и сетевых хранилищ.

### Защита сетевого хранилища EMC группы Celerra / VNX

Kaspersky Security для Windows Server взаимодействует с сетевыми хранилищами EMC группы Celerra / VNX с помощью программного агента CAVA (Celerra Antivirus Agent), работающего на защищаемом устройстве с установленной программой Kaspersky Security для Windows Server. После запуска Kaspersky Security для Windows Server проверяет наличие на защищаемом устройстве установленного агента CAVA, соответствующего требованиям Kaspersky Security для Windows Server.

При попытке чтения или записи в файл, размещенного в сетевом хранилище, сетевое хранилище инициирует сетевой запрос и передает файл агенту CAVA. Агент CAVA записывает полученный файл на локальный диск компьютера в специально созданную папку. Компонент Постоянная защита файлов перехватывает файловую операцию и выполняет проверку файла в соответствии с параметрами, заданными в задаче Постоянная защита файлов, например, лечит или удаляет файл. Агент CAVA анализирует действия Kaspersky Security для Windows Server, формирует результат проверки и передает его в сетевое хранилище.

### Защита RPC-подключаемых сетевых хранилищ

Для взаимодействия Kaspersky Security для Windows Server с RPC-подключаемыми сетевыми хранилищами (такими как NetApp или Hitachi NAS в режиме RPC) используется протокол RPC (Remote Procedure Call).

Kaspersky Security для Windows Server поддерживает постоянное соединение с сетевым хранилищем, периодически инициируя к нему запросы RPC. При попытке чтения, создания или изменения файла, размещенного в сетевом хранилище, сетевое хранилище предоставляет Kaspersky Security для Windows Server прямой доступ к этому файлу по протоколу CIFS. Компонент Защита RPC-подключаемых сетевых хранилищ выполняет проверку файла в соответствии с параметрами, заданными в задаче Защита RPC-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security для Windows Server выполняет над файлом действия, заданные в параметрах задачи (в том числе, лечение или удаление файла), и передает результат проверки сетевому хранилищу.

### Защита ICAP-подключаемых сетевых хранилищ

Для ICAP-подключаемых сетевых хранилищ (таких как EMC Isilon, IBM NAS или Hitachi NAS в режиме ICAP) Kaspersky Security для Windows Server исполняет функции службы, работающей по протоколу ICAP (Internet Content Adaptation Protocol).

При попытке чтения, создания или изменения файла, размещенного в сетевом хранилище, сетевое хранилище формирует ICAP-запрос к Kaspersky Security для Windows Server и передает файл внутри этого запроса. Компонент Защита ICAP-подключаемых сетевых хранилищ выполняет проверку файла в соответствии с параметрами, заданными в задаче Защита ICAP-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security для Windows Server выполняет над файлом действия, заданные в параметрах задачи, и возвращает результат проверки сетевому хранилищу. Если в параметрах задачи выбрано действие Лечить, и файл удалось вылечить, Kaspersky Security для Windows Server возвращает вылеченный файл в сетевое хранилище в ответе на запрос.

## В этом разделе

|                                                                                                   |                     |
|---------------------------------------------------------------------------------------------------|---------------------|
| Настройка входящих и исходящих подключений в брандмауэре Windows .....                            | <a href="#">597</a> |
| Настройка параметров безопасности локальных политик в редакторе локальной групповой политики..... | <a href="#">598</a> |

## Настройка входящих и исходящих подключений в брандмауэре Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► Чтобы настроить входящие и исходящие подключения в брандмауэре Windows, выполните следующие действия:

1. Откройте окно настройки брандмауэра Windows одним из следующих способов:
  - Если вы настраиваете брандмауэр Windows локально, нажмите на кнопку **Пуск**, введите в поисковой строке команду `wf.msc` и нажмите на клавишу **ENTER**.
  - Если вы настраиваете брандмауэр Windows с другого компьютера, выполните следующие действия:
    - a. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.  
Откроется окно **Консоль управления**.
    - b. В открывшемся окне выберите **Файл > Добавить или удалить оснастку**.  
Откроется окно **Добавление и удаление оснасток**.
    - c. В списке доступных оснасток выберите оснастку **Брандмауэр Windows в режиме повышенной безопасности** и нажмите на кнопку **Добавить**.  
Откроется окно **Выбор компьютера**.
    - d. В открывшемся окне выберите вариант **Другой компьютер** и укажите сервер с установленной программой Kaspersky Security для Windows Server одним из следующих способов:
      - В поле ввода укажите доменное имя сервера с установленной программой Kaspersky Security для Windows Server.
      - Нажмите на кнопку **Обзор** и в открывшемся окне выбора встроенного субъекта безопасности выберите сервер с установленной программой Kaspersky Security для Windows Server, используя поиск по домену или рабочей группе.
    - e. Нажмите на кнопку **ОК**.  
Внесенные изменения будут сохранены.
2. Создайте правила для входящих и исходящих подключений со следующими параметрами:

- Разрешите входящие подключения со всех удаленных портов к локальным портам TCP 137 – 139, TCP 445.
- Разрешите исходящие подключения со всех локальных портов к удаленным портам TCP 137 – 139, TCP 445.

Если все исходящие подключения запрещены, откройте следующие порты: TCP 443 (RPC(HTTP)), TCP 445 (SMB), TCP 88 (Kerberos), TCP 53 (DNS), UDP 53 (DNS).

По умолчанию брандмауэр Windows разрешает все входящие соединения, для которых нет запрещающих правил. Если используются параметры по умолчанию, правило для исходящих соединений создавать не требуется.

Параметры брандмауэра Windows могут также определяться групповой или доменной политикой.

## Настройка параметров безопасности локальных политик в редакторе локальной групповой политики

Названия параметров могут отличаться в разных операционных системах Windows.

- Чтобы настроить параметры безопасности локальных политик в редакторе локальной групповой политики, выполните следующие действия:
1. Откройте **Редактор локальной групповой политики** одним из следующих способов:
    - Если вы настраиваете параметры локально, нажмите на кнопку **Пуск**, введите в поисковой строке команду `gpedit.msc` и нажмите на клавишу **ENTER**.
    - Если вы настраиваете параметры с другого компьютера, выполните следующие действия:
      - a. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.  
Откроется окно Консоль управления.
      - b. В открывшемся окне выберите **Файл > Добавить или удалить оснастку**.  
Откроется окно **Добавление и удаление оснасток**.
      - c. В списке доступных оснасток выберите оснастку **Редактор объектов групповой политики** и нажмите на кнопку **Добавить**.  
Запустится **Мастер групповой политики**.
      - d. В окне мастера нажмите на кнопку **Обзор**.  
Откроется окно **Поиск объекта групповой политики**.

- е. В открывшемся окне на закладке **Компьютеры** выберите вариант **Другой компьютер** и укажите сервер с установленной программой Kaspersky Security для Windows Server одним из следующих способов:
    - В поле ввода укажите доменное имя сервера с установленной программой Kaspersky Security для Windows Server.
    - Нажмите на кнопку **Обзор** и в открывшемся окне выбора компьютера выберите сервер с установленной программой Kaspersky Security для Windows Server, используя поиск по домену или рабочей группе.
  - ф. Нажмите на кнопку **ОК**.

Внесенные изменения будут сохранены.
  2. Выберите **Конфигурация компьютера > Параметры Windows > Параметры безопасности > Локальные политики > Параметры безопасности**.
  3. Укажите следующие значения параметров сетевого доступа:
    - **Сетевой доступ: разрешать использование разрешения "Для всех пользователей" для анонимных пользователей** – включено.
    - **Сетевой доступ: не разрешать перечисление учетных записей SAM анонимным пользователям** – выключено.
    - **Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам** – выключено.
  4. Перезагрузите сервер с установленной программой Kaspersky Security для Windows Server.
- Внесенные изменения вступят в силу.

## Работа с Консолью Kaspersky Security для Windows Server

В этом разделе приведена информация о Консоли Kaspersky Security для Windows Server и об управлении Kaspersky Security для Windows Server через Консоль программы, установленную на защищаемом сервере или на другом компьютере.

### В этом разделе

|                                                                         |                     |
|-------------------------------------------------------------------------|---------------------|
| О Консоли Kaspersky Security для Windows Server .....                   | <a href="#">600</a> |
| Запуск Консоли Kaspersky Security для Windows Server из меню Пуск ..... | <a href="#">601</a> |
| Окно Консоли Kaspersky Security для Windows Server .....                | <a href="#">602</a> |
| Просмотр информации о состоянии защиты сетевых хранилищ.....            | <a href="#">605</a> |
| Управление задачами защиты сетевых хранилищ.....                        | <a href="#">607</a> |

## О Консоли Kaspersky Security для Windows Server

Консоль Kaspersky Security для Windows Server представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

После установки Консоли программы на другое устройство требуется дополнительная настройка.

Если Консоль программы и Kaspersky Security для Windows Server установлены на разных защищаемых устройствах, принадлежащих к разным доменам, возможны ограничения в передаче информации от Kaspersky Security для Windows Server на Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Security для Windows Server добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Security для Windows Server или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Security для Windows Server только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.



Можно добавить несколько оснасток Kaspersky Security для Windows Server в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Security для Windows Server.

## Запуск Консоли Kaspersky Security для Windows Server из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► Чтобы запустить Консоль программы из меню **Пуск**, выполните следующие действия:

1. В меню **Пуск** выберите **Программы > Kaspersky Security для Windows Server > Средства администрирования > Консоль Kaspersky Security для Windows Server**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:

1. В меню **Пуск** выберите **Программы > Kaspersky Security для Windows Server > Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.

Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом устройстве откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом устройстве, подключитесь к защищаемому устройству.

► Чтобы подключиться к защищаемому устройству, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
2. Выберите команду **Подключиться к другому компьютеру**.  
Откроется окно **Выбор компьютера**.
3. В открывшемся окне выберите **Другой компьютер**.
4. В поле ввода справа укажите сетевое имя защищаемого устройства.
5. Нажмите на кнопку **ОК**.

Консоль программы подключится к защищаемому устройству.

Если учетная запись, используемая для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на защищаемом устройстве, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

## Окно Консоли Kaspersky Security для Windows Server

Консоль Kaspersky Security для Windows Server отображается в дереве Microsoft Management Console в виде узла с именем Kaspersky Security.

После подключения к программе Kaspersky Security для Windows Server, установленной на другом защищаемом устройстве, в название узла добавляется имя защищаемого устройства, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Security <имя защищаемого устройства> как <имя учетной записи>**. При подключении к программе Kaspersky Security для Windows Server, установленной на том же защищаемом устройстве, что и Консоль программы, узел называется **Kaspersky Security**.

### Дерево Консоли

В дереве Консоли программы отображается узел **Kaspersky Security** и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Security** содержит следующие вложенные узлы:

- **Постоянная защита сервера:** управление задачами постоянной защиты и службами KSN. Узел **Постоянная защита сервера** позволяет настраивать следующие задачи:
  - **Постоянная защита файлов**
  - **Проверка скриптов**
  - **Использование KSN**
  - **Защита трафика**
  - **Защита от шифрования**
- **Контроль сервера:** контроль запуска программ, установленных на защищаемом устройстве, а также контроль подключения внешних устройств. Узел **Контроль сервера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**
- **Автоматическое формирование правил:** настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имена задач>** (если есть)  
Групповые задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль программы.
- **Диагностика системы:** настройка параметров контроля файловых операций и анализа журнала событий Windows.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Защита сетевых хранилищ:** настройка задач защиты сетевых хранилищ.
  - **Защита RPC-подключаемых сетевых хранилищ**
  - **Защита ICAP-подключаемых сетевых хранилищ**

- **Защита от шифрования для NetApp**
- **Проверка по требованию:** управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка объектов на карантине**
  - **Проверка целостности программы**
  - **Мониторинг целостности файлов на основе эталона**
  - Пользовательские задачи **<Имена задач>** (если есть)

В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)), созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Обновление:** управление обновлением баз и модулей Kaspersky Security для Windows Server, а также копированием обновлений в папку локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также последней задачей **Откат обновления баз программы**:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

В узле отображаются все пользовательские и групповые задачи обновления (см. раздел "Категории задач Kaspersky Security для Windows Server" на стр. [160](#)), сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Хранилища:** управление параметрами карантина, резервного хранилища и заблокированных узлов.
  - **Карантин**
  - **Резервное хранилище**
  - **Заблокированные узлы**
- **Журналы и уведомления:** управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Security для Windows Server.
  - **Журнал безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование:** добавление и удаление ключей Kaspersky Security для Windows Server, просмотр информации о лицензиях.

## Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Security**, в панели результатов отображается информация о текущем состоянии защиты устройства (см. раздел "Просмотр состояния защиты и информации о Kaspersky Security для Windows Server" на стр. [172](#)),

информация о Kaspersky Security для Windows Server и о состоянии защиты функциональных компонентов, а также дата истечения срока действия лицензии.

## Контекстное меню узла Kaspersky Security

С помощью пунктов контекстного меню узла **Kaspersky Security** вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру.** Подключиться к другому устройству (см. раздел "Управление Kaspersky Security для Windows Server через Консоль программы на другом устройстве" на стр. [153](#)), чтобы управлять установленной на нем программой Kaspersky Security для Windows Server. Для выполнения этой операции вы можете также воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Security**.
- **Запустить службу / Остановить службу.** Запустить или остановить программу или выбранную задачу (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настроить параметры проверки съемных дисков.** Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. [518](#)), подключенных к защищаемому устройству через USB-порт.
- **Защита от эксплойтов: общие параметры.** Настроить режим защиты от эксплойтов и профилактические действия.
- **Защита от эксплойтов: параметры защиты процессов.** Добавить процессы, которые нужно защитить, и выбрать техники защиты от эксплойтов (см. раздел "Техники защиты от эксплойтов" на стр. [589](#)).
- **Настроить параметры доверенной зоны.** Просмотреть и настроить параметры доверенной зоны (см. раздел "О доверенной зоне" на стр. [562](#)).
- **Изменить права пользователей на управление программой.** Просмотреть и настроить права доступа к функциям Kaspersky Security для Windows Server.
- **Изменить права пользователей на управление службой Kaspersky Security.** Просмотреть и настроить права пользователя на управление службой Kaspersky Security (см. раздел "Настройка прав доступа на управление Kaspersky Security для Windows Server и службой Kaspersky Security" на стр. [287](#)).
- **Иерархическое хранилище.** Настроить способ доступа к HSM-системе (см. раздел "Настройка параметров HSM-системы в Консоли программы" на стр. [592](#)).
- **Экспортировать параметры.** Сохранить параметры программы в конфигурационный XML-файл (см. раздел "Экспорт параметров" на стр. [167](#)). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры.** Импортировать параметры программы из конфигурационного XML-файла (см. раздел "Импорт параметров" на стр. [168](#)). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях.** Перейти к просмотру информации о Kaspersky Security для Windows Server и текущих доступных обновлениях модулей программы.
- **Обновить.** Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Свойства.** Просмотреть и настроить параметры работы Kaspersky Security для Windows Server или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Security** или кнопкой на панели инструментов.

- **Справка.** Перейти к просмотру справки Kaspersky Security для Windows Server. Выполнение этой операции также доступно в контекстных меню задач программы.

## Панель инструментов и контекстное меню задач Kaspersky Security для Windows Server

Вы можете управлять задачами Kaspersky Security для Windows Server с помощью пунктов контекстного меню каждой задачи в дереве Консоли программы.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Запустить / Остановить.** Запустить или остановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Возобновить / Приостановить.** Возобновить или приостановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. [161](#)). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты сервера и задач проверки по требованию.
- **Добавить задачу.** Создать новую пользовательскую задачу (см. раздел "Создание и настройка задачи проверки по требованию" на стр. [542](#)). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения.** Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. [250](#)). Операция доступна для всех задач.
- **Удалить задачу.** Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Шаблоны параметров.** Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. [168](#)). Операция доступна для задачи Постоянная защита файлов и задач проверки по требованию.

## Просмотр информации о состоянии защиты сетевых хранилищ

► Чтобы просмотреть информацию о состоянии защиты сетевых хранилищ,

в дереве Консоли программы выберите узел **Kaspersky Security**.

По умолчанию информация в панели результатов Консоли Kaspersky Security для Windows Server обновляется автоматически:

- каждые 10 секунд при локальном подключении;
- каждые 15 секунд при удаленном подключении.

► Чтобы вручную обновить информацию в узле **Kaspersky Security**,

в контекстном меню узла **Kaspersky Security** выберите пункт **Обновить**.

В панели результатов узла **Kaspersky Security** на закладке **Защита сетевых хранилищ** отображается информация о состоянии защищаемых сетевых хранилищ.

В разделе **Постоянная защита** отображается информация о задачах защиты RPC- и ICAP-подключаемых сетевых хранилищ, а также о состоянии интеграции с хранилищем Celerra / VNX (см. таблицу ниже).

Table 85. Информация о защите сетевых хранилищ

| Раздел Защита сетевых хранилищ                     | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор состояния защиты сетевых хранилищ</b> | <p>Цвет панели с названием раздела является индикатором состояния задач, описанных в разделе. Индикатор может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Зеленый</b> отображается, если выполняются задачи Защита RPC-подключаемых сетевых хранилищ и Защита ICAP-подключаемых сетевых хранилищ.</li> <li>• <b>Желтый</b> отображается, если <ul style="list-style-type: none"> <li>• Выполняется одна из задач: Защита RPC-подключаемых сетевых хранилищ или Защита ICAP-подключаемых сетевых хранилищ.</li> <li>• Обнаружен антивирусный агент Celerra / VNX.</li> </ul> </li> <li>• <b>Красный</b> отображается, если задачи защиты сетевых хранилищ не выполняются и обнаружен антивирусный агент Celerra / VNX.</li> </ul> |
| <b>Защита RPC-подключаемых сетевых хранилищ</b>    | <p><b>Статус задачи</b> – текущее состояние задачи, например, Выполняется или Остановлена.</p> <p><b>Обнаружено</b> – количество вредоносных объектов, обнаруженных в общих папках RPC-подключаемых сетевых хранилищ. Если количество обнаруженных программ превышает 0, значение строки выделяется красным цветом.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Защита ICAP-подключаемых сетевых хранилищ</b>   | <p><b>Статус задачи</b> – текущее состояние задачи, например, Выполняется или Остановлена.</p> <p><b>Обнаружено</b> – количество вредоносных объектов, обнаруженных в общих папках ICAP-подключаемых сетевых хранилищ. Если количество обнаруженных программ превышает 0, значение строки выделяется красным цветом.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Раздел Защита сетевых хранилищ        | Информация                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Интеграция с EMC Celerra / VNX</b> | <p>Возможны следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Антивирусный агент Celerra / VNX не найден.</b> Программе Kaspersky Security для Windows Server не удалось найти программное обеспечение EMC или произошла ошибка в интеграционном коде.</li> <li>• <b>Защита отключена.</b> Программам Kaspersky Security для Windows Server установила соединение с программным обеспечением EMC, но в Kaspersky Security для Windows Server не выполняется задача постоянной защиты файлов.</li> <li>• <b>Защита включена.</b> Программам Kaspersky Security для Windows Server установила соединение с программным обеспечением EMC, и в Kaspersky Security для Windows Server выполняется задача постоянной защиты файлов.</li> </ul> |

В разделе **Защита от шифрования** (см. таблицу ниже) отображается информация о статусе задачи Защита от шифрования для NetApp.

Table 86. Информация о статусе Защиты от шифрования

| Блок Контроль                                   | Информация                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Индикатор состояния Защиты от шифрования</b> | <p>Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• Зеленый цвет панели – задача Защита от шифрования для NetApp выполняется.</li> <li>• Красный цвет панели – задача Защита от шифрования для NetApp не выполняется.</li> </ul> |
| <b>Защита от шифрования для NetApp</b>          | <p><b>Статус задачи</b> – текущее состояние задачи, например, <i>Выполняется</i> или <i>Остановлена</i>.</p> <p><b>Режим</b> – один из двух доступных режимов задачи Защита от шифрования для NetApp.</p> <p><b>Заблокировано узлов</b> – количество скомпрометированных узлов, заблокированных при попытке доступа к общим сетевым папкам на защищаемом сервере.</p>   |

## Управление задачами защиты сетевых хранилищ

В этом разделе приведена информация о задачах Kaspersky Security для Windows Server: их создании, запуске и остановке вручную или автоматически, а также о задании параметров задач.



## В этом разделе

|                                                                        |                     |
|------------------------------------------------------------------------|---------------------|
| Сохранение задачи после изменения ее параметров .....                  | <a href="#">608</a> |
| Запуск / приостановка / возобновление / остановка задачи вручную ..... | <a href="#">608</a> |
| Работа с расписанием задач .....                                       | <a href="#">608</a> |

## Сохранение задачи после изменения ее параметров

Вы можете изменять параметры как выполняемой, так и остановленной (приостановленной) задачи. Новые значения параметров вступят в силу при следующих условиях:

- если вы изменили параметры выполняемой задачи: новые значения параметров применяются сразу после сохранения задачи;
- если вы изменили параметры остановленной (приостановленной) задачи: новые значения параметров применяются при следующем запуске задачи.

### ► Чтобы сохранить измененные параметры задачи,

в контекстном меню названия задачи выберите пункт **Сохранить задачу**.

Если после изменения параметров задачи вы выберете другой узел дерева Консоли программы, не выбрав предварительно команду **Сохранить задачу**, появится окно сохранения параметров.

### ► Чтобы сохранить измененные параметры при переходе к другому узлу Консоли,

в окне сохранения параметров нажмите на кнопку **Да**.

## Запуск / приостановка / возобновление / остановка задачи вручную

### ► Чтобы запустить или остановить задачу защиты сетевых хранилищ, выполните следующие действия:

1. Откройте контекстное меню задачи в Консоли Kaspersky Security для Windows Server.
2. Выберите один из пунктов: **Запустить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита.

## Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Security для Windows Server по расписанию, а также настраивать параметры запуска задач по расписанию.



## В этом разделе

|                                                          |                     |
|----------------------------------------------------------|---------------------|
| Настройка параметров расписания запуска задач .....      | <a href="#">609</a> |
| Включение и выключение запуска задач по расписанию ..... | <a href="#">610</a> |

## Настройка параметров расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Нельзя настроить расписание запуска групповых задач.

► Чтобы настроить расписание запуска задач, выполните следующие действия:

1. Откройте контекстное меню задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.
3. Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.
5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
  - а. В списке **Частота запуска** выберите одно из следующих значений:
    - **Ежечасно**, если требуется запускать задачу с периодичностью в заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч.**
    - **Ежесуточно**, если требуется запускать задачу с периодичностью в заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут.**
    - **Еженедельно**, если требуется запускать задачу с периодичностью в заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед.** Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
    - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Security для Windows Server.
    - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
  - б. В поле **Время запуска** укажите время первого запуска задачи.
  - в. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**. Значение **Запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики Kaspersky Security Center.

6. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
  - В блоке **Дополнительные параметры**:
    - a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
    - b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
    - c. Установите флажок **Распределить время запуска в интервале** и укажите значение в минутах.
7. Нажмите кнопку **Применить**.

Настроенные параметры расписания запуска задачи будут сохранены.

## Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:
  - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
  - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем запуске задачи по расписанию.

4. Нажмите кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

## Защита сетевых хранилищ EMC группы Celerra / VNX

В этом разделе приведена информация о защите сетевых хранилищ EMC группы Celerra / VNX (далее также Celerra / VNX) и об интеграции Kaspersky Security для Windows Server с сетевым хранилищем Celerra / VNX.

### В этом разделе

|                                                                                                     |                     |
|-----------------------------------------------------------------------------------------------------|---------------------|
| О защите сетевых хранилищ EMC группы Celerra / VNX .....                                            | <a href="#">611</a> |
| Интеграция Kaspersky Security для Windows Server с сетевым хранилищем EMC группы Celerra / VNX..... | <a href="#">612</a> |

## О защите сетевых хранилищ EMC группы Celerra / VNX

Программа Kaspersky Security для Windows Server, установленная на сервере с операционной системой Microsoft Windows, защищает сетевые хранилища EMC группы Celerra / VNX от вирусов и других угроз безопасности, проникающих на сервер посредством файлового обмена.

Kaspersky Security для Windows Server проверяет файлы, размещенные в общих сетевых папках в сетевом хранилище EMC группы Celerra / VNX, при попытке чтения или изменения этих файлов с рабочих станций. Сетевое хранилище допускает чтение или изменение файла, если программа Kaspersky Security для Windows Server признала этот файл безопасным. Если Kaspersky Security для Windows Server признал файл зараженным или возможно зараженным, сетевое хранилище запрещает чтение и изменение этого файла.

В Kaspersky Security для Windows Server можно настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

По умолчанию Kaspersky Security для Windows Server выполняет следующие действия:

- лечит зараженные файлы;
- удаляет зараженные файлы, если лечение невозможно;
- помещает возможно зараженные файлы на карантин;
- помещает копию зараженного файла в резервное хранилище перед лечением или удалением этого файла.

Для защиты сетевого хранилища необходимо обеспечить интеграцию Kaspersky Security для Windows Server с сетевым хранилищем Celerra / VNX.

Защита сетевого хранилища Celerra / VNX реализована с помощью задачи Постоянная защита файлов.

Подробная информация о задаче Постоянная защита файлов приведена в *Руководстве администратора Kaspersky Security для Windows Server*.

## Интеграция Kaspersky Security для Windows Server с сетевым хранилищем EMC группы Celerra / VNX

Для защиты сетевого хранилища необходимо обеспечить интеграцию Kaspersky Security для Windows Server с сетевым хранилищем Celerra / VNX.

Интеграция Kaspersky Security для Windows Server с сетевым хранилищем Celerra / VNX выполняется, если соблюдены следующие условия:

1. На защищаемом устройстве с программой Kaspersky Security для Windows Server установлен программный агент CAVA (Celerra Antivirus Agent), входящий в комплект программного обеспечения EMC Celerra / VNX. Kaspersky Security для Windows Server взаимодействует с сетевым хранилищем EMC группы Celerra / VNX с помощью этого программного агента.
2. Запущена задача Постоянная защита файлов.

Подробная информация о задаче Постоянная защита файлов и инструкции по настройке ее параметров приведены в *Руководстве администратора Kaspersky Security для Windows Server*.

Статус интеграции Kaspersky Security для Windows Server (см. раздел "Просмотр информации о состоянии защиты сетевых хранилищ" на стр. [605](#)) с сетевым хранилищем Celerra / VNX отображается в панели результатов узла **Kaspersky Security**.

## Защита RPC-подключаемых сетевых хранилищ

В этом разделе приведена информация о защите RPC-подключаемых сетевых хранилищ, настройке соединения между сетевым хранилищем и Kaspersky Security для Windows Server, а также инструкции по настройке параметров задачи Защита RPC-подключаемых сетевых хранилищ и параметров безопасности в задаче.

### В этом разделе

|                                                                                                              |                     |
|--------------------------------------------------------------------------------------------------------------|---------------------|
| О защите RPC-подключаемых сетевых хранилищ .....                                                             | <a href="#">613</a> |
| О проверке символических ссылок .....                                                                        | <a href="#">614</a> |
| О проверке снимков состояния и других томов и папок, доступных только для чтения .....                       | <a href="#">615</a> |
| Настройка соединения между RPC-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server ..... | <a href="#">615</a> |
| Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ .....                                   | <a href="#">619</a> |
| Уровни безопасности в задаче Защита RPC-подключаемых сетевых хранилищ .....                                  | <a href="#">625</a> |
| Просмотр статистики задачи Защита RPC-подключаемых сетевых хранилищ .....                                    | <a href="#">632</a> |

## О защите RPC-подключаемых сетевых хранилищ

Программа Kaspersky Security для Windows Server, установленная на сервере с операционной системой Microsoft Windows, защищает RPC-подключаемые сетевые хранилища (например, сетевые хранилища NetApp) от вирусов и других угроз компьютерной безопасности, проникающих на сервер посредством файлового обмена.

Kaspersky Security для Windows Server проверяет файлы, размещенные в общих сетевых папках в RPC-подключаемом сетевом хранилище (далее также сетевом хранилище), при попытке чтения или изменения этих файлов с рабочих станций. Сетевое хранилище допускает чтение или изменение файла, если программа Kaspersky Security для Windows Server признала этот файл безопасным. Если программа Kaspersky Security для Windows Server признала файл зараженным или возможно зараженным, сетевое хранилище выполняет действия в соответствии с настроенными параметрами (например, запрещает чтение или изменение файла).

В Kaspersky Security для Windows Server можно настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

По умолчанию Kaspersky Security для Windows Server выполняет следующие действия:

- лечит зараженные файлы;
- удаляет зараженные файлы, если лечение невозможно;
- помещает возможно зараженные файлы на карантин;
- помещает копию зараженного файла в резервное хранилище перед лечением или удалением этого файла.

Вы можете защитить сетевые хранилища с помощью одного сервера с установленной программой Kaspersky Security для Windows Server. Для улучшения быстродействия сетевого хранилища и сервера с

установленной программой Kaspersky Security для Windows Server можно использовать несколько серверов с Kaspersky Security для Windows Server для защиты одного сетевого хранилища. В этом случае сетевое хранилище распределяет нагрузку между присоединенными серверами с установленной программой Kaspersky Security для Windows Server.

Для защиты сетевого хранилища добавьте его в качестве области защиты и настройте соединение между сетевым хранилищем и сервером с установленной программой Kaspersky Security для Windows Server. В Kaspersky Security для Windows Server предусмотрена защита RPC-подключаемых сетевых хранилищ, реализованная в виде задачи с названием Защита RPC-подключаемых сетевых хранилищ.

Задача Защита RPC-подключаемых сетевых хранилищ создается по умолчанию и является системной задачей Kaspersky Security для Windows Server. Нельзя удалить или переименовать эту задачу. Нельзя создать пользовательские задачи защиты RPC-подключаемых сетевых хранилищ.

Можно настроить параметры задачи Защита RPC-подключаемых сетевых хранилищ. Параметры, настроенные в свойствах задачи Защита RPC-подключаемых сетевых хранилищ, применяются ко всем областям защиты, добавленным в задачу. Также можно настраивать параметры безопасности для каждой области защиты.

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security для Windows Server не обеспечивает защиту сетевых хранилищ.

Компонент Защита RPC-подключаемых сетевых хранилищ доступен в составе решения Kaspersky Security для Windows Server для сетевых хранилищ.

Подробная информация о решениях для защиты организации, в состав которых входит Kaspersky Security для Windows Server, приведена в *Руководстве администратора Kaspersky Security для Windows Server*.

## О проверке символических ссылок

*Символическая ссылка* – это специальный тип файла, который содержит указатель на другой объект в форме абсолютного или относительного пути. Символическая ссылка может указывать, например, на объект, который находится в общей сетевой папке другого сетевого хранилища.

Проверка символических ссылок в сетевых хранилищах имеет следующие особенности. Kaspersky Security для Windows Server проверяет файл, на который указывает символическая ссылка, только если этот файл входит в область защиты. Если файл, на который указывает символическая ссылка, находится за пределами области защиты, Kaspersky Security для Windows Server не проверяет этот файл. Если в сетевом хранилище разрешен переход по символической ссылке за пределы папки, в которой находится символическая ссылка, рекомендуется убедиться, что папка назначения входит в область защиты. Например, если разрешен переход по символической ссылке между общими сетевыми папками внутри

защищаемого сетевого хранилища, рекомендуется убедиться, что для всех общих сетевых папок включена функция антивирусной проверки.

## О проверке снимков состояния и других томов и папок, доступных только для чтения

Kaspersky Security для Windows Server проверяет файлы, хранящиеся в снимках состояния (снэпшотах) и других томах и папках, доступных только для чтения, но не выполняет никаких действий над файлами в этих томах и папках, например, не блокирует доступ к зараженным файлам. Чтобы исключить угрозу заражения рабочих станций, рекомендуется делать снимки состояния и другие тома и папки, доступные только для чтения, скрытыми от пользователей и предоставлять доступ к снимкам состояния и другим томам и папкам, доступным только для чтения, через обращение к администратору.

## Настройка соединения между RPC-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security для Windows Server не обеспечивает защиту сетевых хранилищ.

Для защиты RPC-подключаемых сетевых хранилищ необходимо настроить подключение сетевого хранилища к Kaspersky Security для Windows Server.

► Чтобы настроить соединение между сетевым хранилищем и Kaspersky Security для Windows Server, выполните следующие действия:

1. На сервере с установленной программой Kaspersky Security для Windows Server настройте следующие параметры:
  - Добавьте сетевое хранилище в Kaspersky Security для Windows Server (см. раздел "Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security для Windows Server" на стр. [617](#)).
  - В Консоли Kaspersky Security для Windows Server укажите учетную запись, с правами которой вы хотите запускать задачу Защита RPC-подключаемых сетевых хранилищ (см. раздел "Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ" на стр. [616](#)).
  - В редакторе локальной групповой политики настройте параметры безопасности локальных политик (см. раздел "Настройка параметров безопасности локальных политик в редакторе локальной групповой политики" на стр. [598](#)).
  - В окне параметров брандмауэра Windows настройте правила входящих и исходящих подключений в брандмауэре Windows (см. раздел "Настройка входящих и исходящих подключений в брандмауэре Windows" на стр. [597](#)).
  - Если требуется, установите программу-коннектор для RPC-подключаемого сетевого хранилища, защищаемого Kaspersky Security для Windows Server.

Вы можете найти информацию об установке программы-коннектора для защищаемого сетевого хранилища в документации к этому сетевому хранилищу.

2. В сетевом хранилище настройте следующие параметры:

- Включите функцию антивирусной защиты (vscan).
- В группу Backup Operators добавьте учетную запись, с правами которой будет запускаться задача Защита RPC-подключаемых сетевых хранилищ.

Вы можете найти информацию о настройке используемого сетевого хранилища в документации к этому сетевому хранилищу.

Соединение между RPC-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server будет установлено.

## В этом разделе

Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ ..... [616](#)

Формирование области защиты в задаче Защита RPC-подключаемых сетевых хранилищ ..... [617](#)

## Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ

Учетная запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ, должна обладать правами администратора на сервере с установленной программой Kaspersky Security для Windows Server и входить в группу Backup Operators на сетевом хранилище.

Если сетевое хранилище и сервер с установленной программой Kaspersky Security для Windows Server находятся в одном домене, можно использовать доменную учетную запись. Если сетевое хранилище и сервер с установленной программой Kaspersky Security для Windows Server находятся в одной рабочей группе, можно использовать локальные учетные записи с одинаковыми именем пользователя и паролем.

Для сетевых хранилищ, находящихся под управлением операционной системы Data ONTAP 8.2.1 или выше в кластерном режиме, доступно использование только доменной учетной записи.

Если на стороне Kaspersky Security для Windows Server существует несколько учетных записей пользователя, убедитесь, что пользователь, с правами которого выполняется настройка и запуск задачи Защита RPC-подключаемых сетевых хранилищ, добавлен в список пользователей с привилегированным доступом для работы с NetApp. Если учетная запись не обладает необходимыми правами, файлы в папках общего доступа в сетевом хранилище будут доступны, но при выполнении задач защиты проверка этих папок выполняться не будет.



- Чтобы указать учетную запись, с правами которой запускается задача **Защита RPC-подключаемых сетевых хранилищ**, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** и в разделе **Параметры соединения с сетевым хранилищем** введите имя учетной записи, с правами которой запускается задача, пароль этой учетной записи и подтверждение пароля.
5. Нажмите на кнопку **ОК**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

## Формирование области защиты в задаче **Защита RPC-подключаемых сетевых хранилищ**

В этом разделе приведены инструкции по формированию и управлению областью защиты в задаче **Защита RPC-подключаемых сетевых хранилищ**.

### В этом разделе

|                                                                                           |                     |
|-------------------------------------------------------------------------------------------|---------------------|
| Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security для Windows Server . | <a href="#">617</a> |
| Включение и выключение защиты добавленного RPC-подключаемого сетевого хранилища .....     | <a href="#">618</a> |
| Удаление RPC-подключаемого сетевого хранилища из области защиты .....                     | <a href="#">619</a> |

## Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security для Windows Server

- Чтобы добавить RPC-подключаемое сетевое хранилище в область защиты Kaspersky Security для Windows Server, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.

4. В открывшемся окне нажмите на кнопку **Добавить**.

Откроется окно **Добавление области защиты**.

5. В окне **Добавление области защиты** введите доменное имя или IP-адрес сетевого хранилища.

Если вы используете сетевое хранилище NetApp под управлением операционной системы NetApp Clustered Data ONTAP, укажите в этом поле IP-адрес компьютера, на котором установлена программа-коннектор, то есть 127.0.0.1.

6. Нажмите на кнопку **ОК**, чтобы добавить сетевое хранилище в Kaspersky Security для Windows Server.

Сетевое хранилище появится в списке защищаемых сетевых хранилищ.

7. Нажмите на кнопку **Сохранить**.

Настроенные параметры области защиты будут сохранены.

Kaspersky Security для Windows Server подключается к сетевому хранилищу в момент запуска задачи Защита RPC-подключаемых сетевых хранилищ. Если вы указали неправильное доменное имя или неправильный IP-адрес сетевого хранилища, задача завершается с ошибкой. Kaspersky Security для Windows Server записывает информацию об этом событии в журнал системного аудита и в журнал выполнения задачи.

Если вы используете сетевое хранилище NetApp под управлением операционной системы NetApp Clustered Data ONTAP, Kaspersky Security для Windows Server подключается к программе-коннектору, которая установлена на защищаемом сервере. Рекомендуется убедиться, что соединение между программой-коннектором и сетевым хранилищем NetApp настроено правильно и Kaspersky Security для Windows Server защищает добавленное сетевое хранилище.

## Включение и выключение защиты добавленного RPC-подключаемого сетевого хранилища

- Чтобы выключить защиту добавленного RPC-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ снимите флажок рядом с именем сетевого хранилища, для которого вы хотите временно выключить защиту.
5. Нажмите на кнопку **Сохранить**.

Kaspersky Security для Windows Server разорвет соединение с выбранным сетевым хранилищем.

Если вы выключите функцию защиты для всех добавленных сетевых хранилищ, Kaspersky Security для Windows Server остановит выполнение задачи Защита RPC-подключаемых сетевых хранилищ.

- Чтобы включить защиту добавленного RPC-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ установите флажок рядом с именем сетевого хранилища, для которого вы хотите включить защиту.
5. Нажмите на кнопку **Сохранить**.

Если включена защита RPC-подключаемых сетевых хранилищ, Kaspersky Security для Windows Server устанавливает соединение с сетевым хранилищем. Если задача Защита RPC-подключаемых сетевых хранилищ не выполняется, вам нужно запустить ее, чтобы установить соединение Kaspersky Security для Windows Server с сетевым хранилищем.

## Удаление RPC-подключаемого сетевого хранилища из области защиты

- Чтобы удалить RPC-подключаемое сетевое хранилище из задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, которое требуется из области защиты.
5. В контекстном меню имени или IP-адреса сетевого хранилища, которое вы хотите удалить из области защиты, выберите пункт **Удалить из списка**.

Выбранное сетевое хранилище будет удалено из списка защищаемых сетевых хранилищ.

## Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ

По умолчанию в задаче Защита RPC-подключаемых сетевых хранилищ используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

При изменении параметров задачи, например, выборе другой области защиты, Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Kaspersky Security для Windows Server сохранит в журнале системного аудита дату и время изменения параметров задачи.

Table 87. Параметры задачи Защита RPC-подключаемых сетевых хранилищ

| Параметр                                  | Значение по умолчанию                                                                                                                                                                                                                                                                                                                                                                                            | Комментарий                                                                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Область защиты                            | Не доступно.                                                                                                                                                                                                                                                                                                                                                                                                     | Необходимо добавить сетевое хранилище в Kaspersky Security для Windows Server.                                                                                                             |
| Уровень безопасности                      | Применяется уровень безопасности <b>Рекомендуемый</b> .                                                                                                                                                                                                                                                                                                                                                          | Вы можете применить к защищаемому сетевому хранилищу один из стандартных уровней безопасности, или настроить значения параметров безопасности вручную.                                     |
| Эвристический анализатор                  | Применяется уровень анализа Средний.                                                                                                                                                                                                                                                                                                                                                                             | Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.                                                                                        |
| Доверенная зона                           | Применяется.                                                                                                                                                                                                                                                                                                                                                                                                     | Вы можете включать и выключать применение доверенной зоны и настраивать параметры доверенной зоны.                                                                                         |
| Использование KSN                         | Применяется.                                                                                                                                                                                                                                                                                                                                                                                                     | Вы можете включать и выключать использование служб KSN в задаче Защита RPC-подключаемых сетевых хранилищ.                                                                                  |
| Параметры соединения с сетевым хранилищем | <ul style="list-style-type: none"> <li>Имя пользователя и Пароль учетной записи, с правами которой запускается задача – отсутствуют.</li> <li>Промежуток времени между попытками восстановления соединения (сек.): 5.</li> <li>Максимальное количество попыток восстановления соединения: 3.</li> <li>Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы – флажок снят.</li> </ul> | Необходимо указать учетную запись, с правами которой запускается задача Защита RPC-подключаемых сетевых хранилищ. Также можно изменить другие параметры соединения с сетевыми хранилищами. |
| Запуск задачи по расписанию               | Не применяется. Флажок <b>Запускать задачу по расписанию</b> снят. Задача запускается вручную.                                                                                                                                                                                                                                                                                                                   | Вы можете настроить запуск задачи по расписанию, например, при запуске Kaspersky Security для Windows Server.                                                                              |

► Чтобы настроить параметры задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** настройте следующие параметры задачи:
  - Применение эвристического анализатора (см. стр. [621](#)).
  - Запуск задачи с правами учетной записи (см. раздел "Выбор учетной записи для запуска задачи Защита RPC-подключаемых сетевых хранилищ" на стр. [616](#)).
  - Соединение с RPC-подключаемым сетевым хранилищем (см. раздел "Настройка общих параметров соединения с RPC-подключаемым сетевым хранилищем" на стр. [624](#)).
  - Интеграция с другими компонентами Kaspersky Security для Windows Server.
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. [609](#)).
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.  
Изменения параметров задачи будут сохранены.
7. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настройка области защиты**.
8. Выполните следующие действия:
  - Добавьте RPC-подключаемые сетевые хранилища в область защиты Kaspersky Security для Windows Server (см. раздел "Добавление RPC-подключаемого сетевого хранилища в Kaspersky Security для Windows Server" на стр. [617](#)).
  - В списке добавленных сетевых хранилищ, подключаемых по протоколу RPC, выберите сетевые хранилища, защиту которых требуется активировать.
  - Выберите один из стандартных уровней безопасности (см. раздел "Применение стандартного уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ" на стр. [627](#)) или настройте параметры безопасности вручную (см. раздел "Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ" на стр. [627](#)).
9. Нажмите на кнопку **ОК** в окне **Настройка области защиты**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале выполнения задачи.

## В этом разделе

|                                                                                   |                     |
|-----------------------------------------------------------------------------------|---------------------|
| Применение эвристического анализатора .....                                       | <a href="#">621</a> |
| Интеграция с другими компонентами Kaspersky Security для Windows Server .....     | <a href="#">622</a> |
| Настройка общих параметров соединения с RPC-подключаемым сетевым хранилищем ..... | <a href="#">624</a> |

## Применение эвристического анализатора

В задаче Защита RPC-подключаемых сетевых хранилищ можно использовать эвристический анализатор с настроенным уровнем анализа.

- Чтобы настроить параметры использования эвристического анализатора в задаче *Защита RPC-подключаемых сетевых хранилищ*, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в разделе **Эвристический анализатор** выполните следующие действия:
  - Снимите или установите флажок **Использовать эвристический анализатор**.
  - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Интеграция с другими компонентами Kaspersky Security для Windows Server

Задача *Защита RPC-подключаемых сетевых хранилищ* передает в Kaspersky Sandbox только файлы документов.

Вы можете использовать задачу *Защита RPC-подключаемых сетевых хранилищ* совместно со следующими функциональными компонентами и задачами Kaspersky Security для Windows Server:

- Доверенная зона
- Задача Использование KSN

Доверенная зона – это заранее сформированный список исключений из области защиты или проверки.

Вы можете включить или выключить применение доверенной зоны в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите доверенную зону, исключения в ней немедленно начинают или перестают действовать.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ.

Вы можете включить или выключить использование KSN в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите использование KSN, задача начнет или перестанет выносить заключения о репутации проверяемых файлов на основе информации, полученной от KSN.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

► Чтобы включить или выключить использование других компонентов программы в задаче Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в разделе **Интеграция с другими компонентами Kaspersky Security для Windows Server** выполните следующие действия:

- Установите или снимите флажок **Применять доверенную зону**.

Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Security для Windows Server добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Security для Windows Server не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать KSN для защиты**.

Флажок включает или выключает использование служб Kaspersky Security Network (KSN) задачей Защита RPC-подключаемых сетевых хранилищ.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача Защита RPC-подключаемых сетевых хранилищ не использует службы KSN.



По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

## Настройка общих параметров соединения с RPC-подключаемым сетевым хранилищем

- Чтобы настроить общие параметры соединения с RPC-подключаемым сетевым хранилищем, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в разделе Параметры соединения с сетевым хранилищем выполните следующие действия:
  - Укажите период ожидания между попытками восстановления соединения с сетевым хранилищем.
  - Укажите максимальное количество попыток восстановления соединения с сетевым хранилищем.

Рекомендуется оставлять значения, указанные по умолчанию, или указывать большие значения.

- Если требуется, чтобы после каждого обновления баз программы Kaspersky Security для Windows Server очищал кеш проверенных файлов сетевого хранилища, установите флажок



**Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы.**

- Если требуется, чтобы после каждого обновления баз программы Kaspersky Security для Windows Server сохранял кеш проверенных файлов сетевого хранилища, снимите флажок **Очищать кеш проверенных файлов сетевого хранилища после обновления баз программы.**

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

## Уровни безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

В этом разделе описаны параметры безопасности и приведены инструкции по применению стандартных уровней безопасности и настройке параметров безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ.

### В этом разделе

|                                                                                                           |                     |
|-----------------------------------------------------------------------------------------------------------|---------------------|
| Об уровнях безопасности в задаче Защита RPC-подключаемых сетевых хранилищ .....                           | <a href="#">625</a> |
| Применение стандартного уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ .....       | <a href="#">627</a> |
| Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ .....  | <a href="#">627</a> |
| Работа с шаблонами параметров уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ ..... | <a href="#">629</a> |

## Об уровнях безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

В задаче Защита RPC-подключаемых сетевых хранилищ для каждого защищаемого хранилища вы можете применить один из следующих стандартных уровней безопасности: **Максимальное быстроедействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней безопасности имеет свой набор параметров безопасности (см. Таблицу ниже). Вы также можете настроить значения параметров безопасности вручную, уровень безопасности для сетевого хранилища в этом случае изменится на **Пользовательский**.

### Максимальное быстроедействие

Уровень безопасности **Максимальное быстроедействие** рекомендуется применять, если, кроме использования Kaspersky Security для Windows Server на серверах и рабочих станциях, в вашей сети применяются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

### Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых серверов. Этот уровень рекомендован специалистами

"Лаборатории Касперского", как достаточный для защиты файловых серверов в большинстве сетей организаций. Уровень безопасности Рекомендуемый установлен по умолчанию.

### Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

Table 88. Параметры стандартных уровней безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

| Параметры                                            | Уровень безопасности                                                       |                                                                                                                          |                                                                                                                          |
|------------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
|                                                      | Максимальное быстроедействие                                               | Рекомендуемый                                                                                                            | Максимальная защита                                                                                                      |
| Защита объектов                                      | Объекты, проверяемые по списку расширений, указанному в антивирусных базах | Объекты, проверяемые по формату                                                                                          | Объекты, проверяемые по формату                                                                                          |
| Защита составных объектов                            | Упакованные объекты                                                        | <ul style="list-style-type: none"> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> | <ul style="list-style-type: none"> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> |
| Действия над зараженными объектами                   | Блокировать доступ и лечить. Удалять, если лечение невозможно              | Блокировать доступ и выполнить рекомендуемое действие.                                                                   | Блокировать доступ и лечить. Удалять, если лечение невозможно                                                            |
| Действия над возможно зараженными объектами          | Блокировать доступ и поместить на карантин.                                | Блокировать доступ и выполнить рекомендуемое действие.                                                                   | Блокировать доступ и поместить на карантин.                                                                              |
| Действия в зависимости от типа обнаруженного объекта | Нет                                                                        | Нет                                                                                                                      | Нет                                                                                                                      |
| Исключать файлы                                      | Нет                                                                        | Нет                                                                                                                      | Нет                                                                                                                      |
| Не обнаруживать                                      | Нет                                                                        | Нет                                                                                                                      | Нет                                                                                                                      |
| Останавливать проверку, если она длится более (сек)  | 60                                                                         | 60                                                                                                                       | 60                                                                                                                       |
| Не проверять составные объекты размером более (МБ)   | 8                                                                          | 8                                                                                                                        | Нет                                                                                                                      |

## Применение стандартного уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

► Чтобы применить один из стандартных уровней безопасности для RPC-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, для которого вы требуется выбрать стандартный уровень безопасности.
5. На закладке **Уровень безопасности** выберите в списке один из следующих стандартных уровней безопасности:
  - **Максимальная защита**
  - **Рекомендуемый**
  - **Максимальное быстродействие**

На закладке **Уровень безопасности** отображаются основные значения параметров выбранного уровня безопасности. Применяемый уровень безопасности отображается рядом с именем сетевого хранилища в списке защищаемых сетевых хранилищ.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры уровня безопасности будут сохранены и применены в выполняющейся задаче.

Можно также настроить параметры безопасности защищаемого сетевого хранилища вручную (см. раздел "Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ" на стр. [627](#)).

## Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ

► Чтобы вручную настроить параметры безопасности для RPC-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита RPC-подключаемых сетевых хранилищ** перейдите по ссылке **Настроить область защиты**.
4. В списке защищаемых сетевых хранилищ выберите сетевое хранилище, параметры безопасности которого вы хотите настроить.

Вы можете применить предварительно созданный шаблон параметров безопасности.

5. Настройте параметры для выбранного сетевого хранилища в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:

- На закладке **Общие** выполните следующие действия:
    - В разделе **Защита объектов** укажите объекты, которые будет проверять Kaspersky Security для Windows Server:
      - **Все объекты**  
Kaspersky Security для Windows Server проверяет все объекты.
      - **Объекты, проверяемые по формату**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.  
Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
      - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.  
Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
      - **Объекты, проверяемые по указанному списку расширений**  
Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.
- Этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.
- В разделе **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security для Windows Server.
  - На закладке **Действия** выполните следующие действия:
    - В разделе **Действия над зараженными и другими обнаруженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении зараженного объекта.
    - В разделе **Действия над возможно зараженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении возможно зараженного объекта.
    - Настройте действия над объектами в зависимости от типа обнаруженного объекта.
    - Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

- На закладке **Производительность** выполните следующие действия:
  - В разделе **Исключения** укажите, какие объекты Kaspersky Security для Windows Server исключает из проверки:
    - Чтобы исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
    - Чтобы исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии <http://www.securelist.ru>.
  - В разделе **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.

Если вы используете сетевое хранилище, работающее под управлением операционной системы Clustered Data ONTAP, этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.

## 6. Нажмите на кнопку **Сохранить**.

Настроенные параметры пользовательского уровня безопасности будут сохранены и применены в выполняющейся задаче.

## Работа с шаблонами параметров уровня безопасности в задаче Защита RPC-подключаемых сетевых хранилищ

В этом разделе приведены инструкции по управлению шаблонами параметров уровней безопасности в задаче Защита RPC-подключаемых сетевых хранилищ.

## В этом разделе

|                                                  |                     |
|--------------------------------------------------|---------------------|
| Создание шаблона параметров безопасности .....   | <a href="#">630</a> |
| Применение шаблона параметров безопасности ..... | <a href="#">630</a> |
| Просмотр параметров безопасности в шаблоне ..... | <a href="#">631</a> |
| Удаление шаблона параметров безопасности .....   | <a href="#">631</a> |

## Создание шаблона параметров безопасности

► Чтобы сохранить параметры безопасности узла вручную в шаблон, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для которой вы хотите создать шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.  
Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите дополнительную информацию о шаблоне.
7. Нажмите на кнопку **ОК**.

Шаблон с набором значений параметров безопасности будет сохранен.

## Применение шаблона параметров безопасности

► Чтобы применить параметры безопасности из шаблона для выбранного узла, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты**.
3. В списке сетевых файловых ресурсов сервера выберите узел, к которому вы хотите применить шаблон.
4. В контекстном меню выберите пункт **Применить шаблон**.
5. Выберите **<Название шаблона>**.
6. В дереве Консоли программы откройте контекстное меню настраиваемой задачи.
7. Выберите пункт **Сохранить задачу**.

Шаблон параметров безопасности будет применен к выбранному элементу в дереве файловых ресурсов сервера. На закладке **Уровень безопасности** выбранного элемента будет установлено значение **Пользовательский**.

## Просмотр параметров безопасности в шаблоне

► *Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, шаблон безопасности которой требуется просмотреть.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.  
Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Название шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приведен список значений параметров безопасности, сохраненных в шаблоне.

## Удаление шаблона параметров безопасности

► *Чтобы удалить шаблон параметров безопасности, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для настройки которой больше не требуется использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.  
Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Откроется окно подтверждения операции удаления.

5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов файловых ресурсов сервера, настроенные параметры безопасности для этих узлов сохраняются после удаления шаблона.

## Просмотр статистики задачи Защита RPC-подключаемых сетевых хранилищ

Если задача Защита RPC-подключаемых сетевых хранилищ выполняется, вы можете в реальном времени просматривать информацию о количестве объектов, обработанных программой Kaspersky Security для Windows Server с момента запуска задачи по текущий момент, то есть статистику задачи.

► Чтобы просмотреть статистику задачи Защита RPC-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита RPC-подключаемых сетевых хранилищ**.

В разделе **Статистика** на панели результатов отобразится таблица, содержащая информацию об объектах, обработанных программой Kaspersky Security для Windows Server с момента запуска задачи по текущий момент (см. таблицу ниже).

Table 89. Полная статистика задачи Защита RPC-подключаемых сетевых хранилищ

| Поле                                               | Описание                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обнаружено</b>                                  | Количество объектов, которые обнаружила программа Kaspersky Security для Windows Server. Например, если программа Kaspersky Security для Windows Server обнаружила одну программу в пяти файлах, значение в этом поле увеличится на единицу.                                                                                            |
| <b>Зараженных и других обнаруживаемых объектов</b> | Количество объектов, которые программа Kaspersky Security для Windows Server признала зараженными, или количество обнаруженных файлов легальных программ, которые не были исключены из области действия задач постоянной защиты или проверки по требованию, но могут быть использованы злоумышленниками для нанесения вреда компьютеру. |
| <b>Возможно зараженных объектов</b>                | Количество объектов, которые программа Kaspersky Security для Windows Server признала возможно зараженными.                                                                                                                                                                                                                             |
| <b>Объектов не вылечено</b>                        | Количество объектов, которые программа Kaspersky Security для Windows Server не вылечила по следующим причинам: <ul style="list-style-type: none"> <li>• тип обнаруженного объекта не предполагает лечения;</li> <li>• при лечении возникла ошибка.</li> </ul>                                                                          |
| <b>Объектов не помещено на карантин</b>            | Количество объектов, которые программа Kaspersky Security для Windows Server попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.                                                                                                                                              |
| <b>Объектов не удалено</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.                                                                                                                                                     |
| <b>Объектов не проверено</b>                       | Количество объектов в области защиты, которые программе Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.                                                                                                                                                 |



| Поле                                                 | Описание                                                                                                                                                                                                   |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Объектов, не помещенных в резервное хранилище</b> | Количество объектов, копии которых программа Kaspersky Security для Windows Server попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. |
| <b>Ошибок обработки</b>                              | Количество объектов, во время обработки которых возникла ошибка задачи.                                                                                                                                    |
| <b>Вылечено объектов</b>                             | Количество объектов, которые вылечила программа Kaspersky Security для Windows Server.                                                                                                                     |
| <b>Помещено на карантин</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server поместила на карантин.                                                                                                        |
| <b>Помещено в резервное хранилище</b>                | Количество объектов, копии которых программа Kaspersky Security для Windows Server сохранила в резервном хранилище.                                                                                        |
| <b>Удалено объектов</b>                              | Количество объектов, которые удалила программа Kaspersky Security для Windows Server.                                                                                                                      |
| <b>Защищенных паролем объектов</b>                   | Количество объектов (например, архивов), которые программа Kaspersky Security для Windows Server пропустила, так как эти объекты защищены паролем.                                                         |
| <b>Поврежденных объектов</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server пропустила, так как их формат был искажен.                                                                                    |
| <b>Обработано объектов</b>                           | Общее количество объектов, которые обработала программа Kaspersky Security для Windows Server.                                                                                                             |

## Защита ICAP-подключаемых сетевых хранилищ

В этом разделе приведена информация о задаче защиты ICAP-подключаемых сетевых хранилищ и о подключении сетевого хранилища к Kaspersky Security для Windows Server, а также инструкции по настройке параметров задачи защиты и параметров безопасности ICAP-подключаемых сетевых хранилищ.

### В этом разделе

|                                                                                                              |                     |
|--------------------------------------------------------------------------------------------------------------|---------------------|
| О защите ICAP-подключаемых сетевых хранилищ .....                                                            | <a href="#">634</a> |
| Настройка соединения между ICAP-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server..... | <a href="#">635</a> |
| Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ.....                                   | <a href="#">636</a> |
| Уровни безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ .....                                 | <a href="#">641</a> |
| Просмотр статистики задачи Защита ICAP-подключаемых сетевых хранилищ.....                                    | <a href="#">646</a> |

## О защите ICAP-подключаемых сетевых хранилищ

Программа Kaspersky Security для Windows Server, установленная на сервере с операционной системой Microsoft Windows, защищает ICAP-подключаемые сетевые хранилища (например, EMC Isilon) от вирусов и других угроз безопасности, проникающих на сервер посредством файлового обмена.

Kaspersky Security для Windows Server не имеет прямого доступа к файлам в ICAP-подключаемом сетевом хранилище (далее также *сетевом хранилище*). При попытке чтения или изменения файла, сетевое хранилище формирует ICAP-запрос к Kaspersky Security для Windows Server и передает файл внутри этого запроса. Программа выполняет антивирусную проверку файла в соответствии с параметрами, заданными в задаче Защита ICAP-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security для Windows Server выполняет над файлом действия, заданные в параметрах задачи, и передает результат проверки сетевому хранилищу. Если в параметрах задачи выбрано действие Лечить, и файл удалось вылечить, Kaspersky Security для Windows Server возвращает вылеченный файл в сетевое хранилище в ответе на запрос.

В Kaspersky Security для Windows Server можно настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

При использовании KSN в задаче Защита ICAP-подключаемых сетевых хранилищ, Kaspersky Security для Windows Server не может удалять или блокировать файлы, которые используются ICAP-подключаемым сетевым хранилищем, поскольку программа не имеет прямого доступа к сетевым папкам хранилища при получении от служб KSN заключения о том, что файл является недоверенным. Информация о получении заключения о том, что файл является недоверенным, фиксируется в журнале выполнения задачи Использование KSN.

Одно сетевое хранилище можно защитить с помощью одного сервера с установленной программой Kaspersky Security для Windows Server. Для улучшения быстродействия сетевого хранилища и сервера с

установленной программой Kaspersky Security для Windows Server можно использовать несколько серверов с Kaspersky Security для Windows Server для защиты одного сетевого хранилища. В этом случае сетевое хранилище распределяет нагрузку между присоединенными серверами с установленной программой Kaspersky Security для Windows Server.

Задача Защита ICAP-подключаемых сетевых хранилищ создается по умолчанию и является системной задачей Kaspersky Security для Windows Server. Нельзя удалить или переименовать эту задачу. Нельзя создать пользовательские задачи защиты ICAP-подключаемых сетевых хранилищ. Можно настроить параметры задачи Защита ICAP-подключаемых сетевых хранилищ.

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security для Windows Server не обеспечивает защиту сетевых хранилищ.

Компонент Защита ICAP-подключаемых сетевых хранилищ доступен в составе решения Kaspersky Security для Windows Server для сетевых хранилищ.

Подробная информация о решениях для защиты организации, в состав которых входит Kaspersky Security для Windows Server, приведена в *Руководстве администратора Kaspersky Security для Windows Server*.

## Настройка соединения между ICAP-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security для Windows Server не обеспечивает защиту сетевых хранилищ.

Для защиты ICAP-подключаемых сетевых хранилищ необходимо настроить подключение сетевого хранилища к Kaspersky Security для Windows Server.

► Чтобы настроить соединение между сетевым хранилищем и Kaspersky Security для Windows Server, выполните следующие действия:

1. На сервере с установленной программой Kaspersky Security для Windows Server настройте следующие параметры:

- В Консоли программы укажите параметры соединения с ICAP-подключаемым сетевым хранилищем (см. раздел "Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем" на стр. [638](#)), защищаемым Kaspersky Security для Windows Server.
  - В редакторе локальной групповой политики настройте параметры безопасности локальных политик (см. раздел "Настройка параметров безопасности локальных политик в редакторе локальной групповой политики" на стр. [598](#)).
  - В окне параметров брандмауэра Windows настройте правила входящих и исходящих подключений в брандмауэре Windows (см. раздел "Настройка входящих и исходящих подключений в брандмауэре Windows" на стр. [597](#)).
2. В сетевом хранилище настройте следующие параметры:
- Включите антивирусную защиту.
  - Укажите адрес подключения к Kaspersky Security для Windows Server в параметрах сетевого хранилища.

Вы можете найти информацию о настройке используемого сетевого хранилища в документации к этому сетевому хранилищу.

Соединение между ICAP-подключаемым сетевым хранилищем и Kaspersky Security для Windows Server будет установлено.

## Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ

По умолчанию в задаче Защита ICAP-подключаемых сетевых хранилищ используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

При изменении параметров задачи, например, выборе другого уровня безопасности, Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Kaspersky Security для Windows Server сохранит в журнале системного аудита дату и время изменения параметров задачи.

Table 90. Параметры задачи Защита ICAP-подключаемых сетевых хранилищ

| Параметр                                  | Значение по умолчанию                                                                                                                | Комментарий                                                                                                                                            |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Уровень безопасности                      | Применяется уровень безопасности <b>Рекомендуемый</b> .                                                                              | Вы можете применить к защищаемому сетевому хранилищу один из стандартных уровней безопасности, или настроить значения параметров безопасности вручную. |
| Эвристический анализатор                  | Применяется уровень анализа <b>Средний</b> .                                                                                         | Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.                                                    |
| Использование KSN для защиты              | Применяется.                                                                                                                         | Вы можете включать и выключать использование служб KSN для защиты ICAP-подключаемых сетевых хранилищ.                                                  |
| Параметры соединения с сетевым хранилищем | <ul style="list-style-type: none"> <li><b>Номер сетевого порта</b> – 1344.</li> <li><b>Идентификатор службы</b> – avscan.</li> </ul> | Также можно изменить другие параметры соединения с сетевыми хранилищами. Эти изменения должны быть учтены на сетевых хранилищах.                       |
| Запуск задачи по расписанию               | Не применяется. Флажок <b>Запускать задачу по расписанию</b> снят. Задача запускается вручную.                                       | Вы можете настроить запуск задачи по расписанию, например, при запуске Kaspersky Security для Windows Server.                                          |

► Чтобы настроить параметры задачи Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** настройте следующие параметры задачи:
  - Соединение с ICAP-подключаемым сетевым хранилищем (см. раздел "Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем" на стр. [638](#)).
  - Применение эвристического анализатора (см. стр. [639](#)).
  - Использование KSN для защиты (см. раздел "Использование KSN для защиты" на стр. [639](#)).

В разделе **Уровень безопасности**:

- Выберите один из стандартных уровней безопасности (см. раздел "Об уровнях безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ" на стр. [641](#)) или настройте параметры безопасности вручную (см. раздел "Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ" на стр. [644](#)).
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. [608](#)).

6. Нажмите на кнопку **ОК**.

Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале выполнения задачи.

## В этом разделе

|                                                                             |                     |
|-----------------------------------------------------------------------------|---------------------|
| Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем..... | <a href="#">638</a> |
| Применение эвристического анализатора .....                                 | <a href="#">639</a> |
| Использование KSN для защиты .....                                          | <a href="#">639</a> |
| Использование Kaspersky Sandbox для защиты.....                             | <a href="#">640</a> |

## Настройка параметров соединения с ICAP-подключаемым сетевым хранилищем

► Чтобы настроить параметры соединения с ICAP-подключаемым сетевым хранилищем, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. На закладке **Общие** в полях раздела **Параметры соединения** укажите следующие параметры:

- **Номер сетевого порта**

Номер сетевого порта ICAP-сервера, используемый для подключения сетевого хранилища к программе.

- **Идентификатор службы**

Идентификатор, который является частью параметра RESPMOD URI протокола ICAP (см. документ RFC 3507). RESPMOD URI обозначает адрес антивирусного ICAP-сервера, установленный для сетевого хранилища.

Например, если IP-адрес защищаемого сервера – 192.168.10.10, номер порта – 1344, а идентификатор службы ICAP – avscan, то эти параметры сформируют следующий адрес RESPMOD URI: `icap://192.168.10.10/avscan:1344`.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

После того, как вы настроили параметры соединения, в сетевом хранилище необходимо указать адрес подключения к Kaspersky Security для Windows Server. Параметры соединения включаются в этот адрес. Например, при значениях параметров, заданных по умолчанию, адрес подключения имеет следующий вид:

```
icap://<IP-адрес компьютера с Kaspersky Security для Windows
Server>/avscan:1344
```

## Применение эвристического анализатора

В задаче Защита ICAP-подключаемых сетевых хранилищ можно использовать эвристический анализатор с настроенным уровнем анализа.

► Чтобы настроить параметры использования эвристического анализатора в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** в разделе **Эвристический анализатор** выполните следующие действия:
  - Снимите или установите флажок **Использовать эвристический анализатор**.
  - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".  
Этот уровень выбран по умолчанию.
- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

## Использование KSN для защиты

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ.

Вы можете включить или выключить использование KSN в задаче Защита RPC-подключаемых сетевых хранилищ. После того как вы включите или выключите использование KSN, задача начнет или перестанет выносить заключения о репутации проверяемых файлов на основе информации, полученной от KSN.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network. По умолчанию задача Использование KSN не запускается автоматически при запуске Kaspersky Security для Windows Server.

► Чтобы включить или отключить использование KSN в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:

1. Разверните узел **Защита сетевых хранилищ** в дереве Консоли программы.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** установите или снимите флажок **Использовать KSN для защиты**.

Флажок включает или выключает использование служб Kaspersky Security Network (KSN) задачей Защита ICAP-подключаемых сетевых хранилищ.

Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача Защита ICAP-подключаемых сетевых хранилищ не использует службы KSN.

По умолчанию флажок установлен.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

## Использование Kaspersky Sandbox для защиты

Задача Защита ICAP-подключаемых сетевых хранилищ передает в *Kaspersky Sandbox* только файлы документов.

*Kaspersky Sandbox* – это решение для обнаружения и блокировки комплексных угроз. Виртуальные образы операционных систем разворачиваются на серверах Kaspersky Sandbox, а проверяемые объекты исполняются внутри этих операционных систем. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

► Чтобы включить или отключить использование Kaspersky Sandbox в задаче Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:

1. Разверните узел **Защита сетевых хранилищ** в дереве Консоли программы.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.



3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. В открывшемся окне перейдите на закладку **Общие** и установите или снимите флажок **Использовать Kaspersky Sandbox для защиты**.

Этот флажок включает или выключает использование Kaspersky Sandbox.

Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак.

Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox.

По умолчанию флажок установлен.

Функция Kaspersky Sandbox не работает, если Kaspersky Endpoint Agent не установлен (см. раздел "Установка Kaspersky Security для Windows Server" на стр. [46](#)) на защищаемом устройстве.

Запущенная задача Защита трафика может препятствовать использованию Kaspersky Sandbox. Для использования задачи Защита трафика и Kaspersky Sandbox на одном защищаемом устройстве, перезапустите задачу Защита трафика после установки Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

## Уровни безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

В этом разделе описаны параметры безопасности и приведены инструкции по применению стандартных уровней безопасности и настройке параметров безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ.

### В этом разделе

|                                                                                                           |                     |
|-----------------------------------------------------------------------------------------------------------|---------------------|
| Об уровнях безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ .....                          | <a href="#">641</a> |
| Применение стандартного уровня безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ .....      | <a href="#">643</a> |
| Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ ..... | <a href="#">644</a> |

## Об уровнях безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

В задаче Защита ICAP-подключаемых сетевых хранилищ для каждого защищаемого хранилища вы можете применить один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже). Вы также можете настроить значения параметров

безопасности вручную, уровень безопасности для сетевого хранилища в этом случае изменится на **Пользовательский**.

### Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если, кроме использования Kaspersky Security для Windows Server на серверах и рабочих станциях, в вашей сети применяются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

### Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых серверов. Этот уровень рекомендован специалистами "Лаборатории Касперского", как достаточный для защиты файловых серверов в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

### Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

Table 91. Параметры стандартных уровней безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

| Параметры                                                         | Уровень безопасности                                                       |                                                                                                                          |                                                                                                                          |
|-------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
|                                                                   | Максимальное быстродействие                                                | Рекомендуемый                                                                                                            | Максимальная защита                                                                                                      |
| <b>Защита объектов</b>                                            | Объекты, проверяемые по списку расширений, указанному в антивирусных базах | Объекты, проверяемые по формату                                                                                          | Объекты, проверяемые по формату                                                                                          |
| <b>Защита составных объектов</b>                                  | Упакованные объекты                                                        | <ul style="list-style-type: none"> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> | <ul style="list-style-type: none"> <li>SFX-архивы</li> <li>Упакованные объекты</li> <li>Вложенные OLE-объекты</li> </ul> |
| <b>Действия над зараженными и другими обнаруженными объектами</b> | Лечить                                                                     | Выполнять рекомендованное действие                                                                                       | Лечить                                                                                                                   |

| Параметры                                           | Уровень безопасности        |                                    |                     |
|-----------------------------------------------------|-----------------------------|------------------------------------|---------------------|
|                                                     | Максимальное быстродействие | Рекомендуемый                      | Максимальная защита |
| Действия над возможно зараженными объектами         | Карантин                    | Выполнять рекомендованное действие | Карантин            |
| Исключать файлы                                     | Нет                         | Нет                                | Нет                 |
| Не обнаруживать                                     | Нет                         | Нет                                | Нет                 |
| Останавливать проверку, если она длится более (сек) | 60                          | 60                                 | 60                  |
| Не проверять составные объекты размером более (МБ)  | 8                           | 8                                  | Нет                 |

## Применение стандартного уровня безопасности в задаче Защита ICAP-подключаемых сетевых хранилищ

► Чтобы применить один из стандартных уровней безопасности для ICAP-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. На закладке **Общие** в разделе **Уровень безопасности** выберите в списке один из следующих стандартных уровней безопасности:
  - **Максимальная защита**
  - **Рекомендуемый**
  - **Максимальное быстродействие**

Основные значения параметров выбранного уровня безопасности отображаются под списком.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Можно также настроить параметры безопасности защищаемого сетевого хранилища вручную (см. раздел "Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ" на стр. [644](#)).

## Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ

► Чтобы вручную настроить параметры безопасности для ICAP-подключаемого сетевого хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.
3. В панели результатов узла **Защита ICAP-подключаемых сетевых хранилищ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. На закладке **Общие** в разделе **Уровень безопасности** нажмите на кнопку **Настройка**.

Откроется окно **Параметры безопасности**.

5. Настройте параметры в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:

- На закладке **Общие** выполните следующие действия:
  - В разделе **Защита объектов** укажите объекты, которые будет проверять Kaspersky Security для Windows Server:

- **Все объекты**

Kaspersky Security для Windows Server проверяет все объекты.

- **Объекты, проверяемые по формату**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.

- **Объекты, проверяемые по указанному списку расширений**

Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

Этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.

- В разделе **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security для Windows Server.
  - На закладке **Действия** выполните следующие действия:
    - В разделе **Действия над зараженными и другими обнаруженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении зараженного объекта.
    - В разделе **Действия над возможно зараженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении возможно зараженного объекта.
    - Настройте действия над объектами в зависимости от типа обнаруженного объекта.
  - На закладке **Производительность** выполните следующие действия:
    - В разделе **Исключения** укажите, какие объекты Kaspersky Security для Windows Server исключает из проверки:
      - Чтобы исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
      - Чтобы исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии <https://encyclopedia.kaspersky.ru/knowledge/classification/>.
    - В разделе **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.
6. В окне **Параметры безопасности** нажмите на кнопку **ОК**.  
Окно **Параметры безопасности** закроется.
7. В окне **Параметры задачи** нажмите на кнопку **ОК**.  
Настроенные параметры пользовательского уровня безопасности будут сохранены.

## Просмотр статистики задачи Защита ICAP-подключаемых сетевых хранилищ

Если задача Защита ICAP-подключаемых сетевых хранилищ выполняется, вы можете в реальном времени просматривать информацию о количестве объектов, обработанных программой Kaspersky Security для Windows Server с момента запуска задачи по текущий момент, то есть статистику задачи.

► Чтобы просмотреть статистику задачи Защита ICAP-подключаемых сетевых хранилищ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита ICAP-подключаемых сетевых хранилищ**.

В разделе **Статистика** на панели результатов отобразится таблица, содержащая информацию об объектах, обработанных программой Kaspersky Security для Windows Server с момента запуска задачи по текущий момент (см. таблицу ниже).

Table 92. Статистика задачи Защита ICAP-подключаемых сетевых хранилищ

| Поле                                               | Описание                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обнаружено</b>                                  | Количество объектов, которые обнаружила программа Kaspersky Security для Windows Server. Например, если программа Kaspersky Security для Windows Server обнаружила одну вредоносную программу в пяти файлах, значение в этом поле увеличится на единицу.                                                                                |
| <b>Зараженных и других обнаруживаемых объектов</b> | Количество объектов, которые программа Kaspersky Security для Windows Server признала зараженными, или количество обнаруженных файлов легальных программ, которые не были исключены из области действия задач постоянной защиты или проверки по требованию, но могут быть использованы злоумышленниками для нанесения вреда компьютеру. |
| <b>Возможно зараженных объектов</b>                | Количество объектов, которые программа Kaspersky Security для Windows Server признала возможно зараженными.                                                                                                                                                                                                                             |
| <b>Объектов не вылечено</b>                        | Количество объектов, которые программа Kaspersky Security для Windows Server не вылечила по следующим причинам: <ul style="list-style-type: none"> <li>• тип обнаруженного объекта не предполагает лечения;</li> <li>• При лечении возникла ошибка.</li> </ul>                                                                          |
| <b>Объектов не помещено на карантин</b>            | Количество объектов, которые программа Kaspersky Security для Windows Server попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.                                                                                                                                              |
| <b>Объектов не удалено</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.                                                                                                                                                     |
| <b>Объектов не проверено</b>                       | Количество объектов в области защиты, которые программе Kaspersky Security для Windows Server не удалось проверить, например, если доступ к объекту был заблокирован другой программой.                                                                                                                                                 |

| Поле                                                 | Описание                                                                                                                                                                                                   |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Объектов, не помещенных в резервное хранилище</b> | Количество объектов, копии которых программа Kaspersky Security для Windows Server попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. |
| <b>Ошибок обработки</b>                              | Количество объектов, во время обработки которых возникла ошибка задачи.                                                                                                                                    |
| <b>Вылечено объектов</b>                             | Количество объектов, которые вылечила программа Kaspersky Security для Windows Server.                                                                                                                     |
| <b>Помещено на карантин</b>                          | Количество объектов, которые программа Kaspersky Security для Windows Server поместила на карантин.                                                                                                        |
| <b>Помещено в резервное хранилище</b>                | Количество объектов, копии которых программа Kaspersky Security для Windows Server сохранила в резервном хранилище.                                                                                        |
| <b>Удалено объектов</b>                              | Количество объектов, которые удалила программа Kaspersky Security для Windows Server.                                                                                                                      |
| <b>Защищенных паролем объектов</b>                   | Количество объектов (например, архивов), которые программа Kaspersky Security для Windows Server пропустила, так как эти объекты защищены паролем.                                                         |
| <b>Поврежденных объектов</b>                         | Количество объектов, которые программа Kaspersky Security для Windows Server пропустила, так как их формат был искажен.                                                                                    |
| <b>Обработано объектов</b>                           | Общее количество объектов, которые обработала программа Kaspersky Security для Windows Server.                                                                                                             |

## Защита от шифрования для NetApp

Этот раздел содержит информацию о задаче Защита от шифрования для NetApp и инструкции по настройке ее параметров.

### В этом разделе

|                                                                  |                     |
|------------------------------------------------------------------|---------------------|
| О задаче Защита от шифрования для NetApp.....                    | <a href="#">648</a> |
| Создание и настройка FPolicy .....                               | <a href="#">649</a> |
| Настройка Kaspersky Security для Windows Server.....             | <a href="#">652</a> |
| Настройка параметров задачи Защита от шифрования для NetApp..... | <a href="#">655</a> |

## О задаче Защита от шифрования для NetApp

Защита от шифрования для NetApp обеспечивает защиту от шифрования для папок в сетевых хранилищах. При обнаружении попытки вредоносного шифрования Kaspersky Security для Windows Server блокирует доступ к папкам защищаемого сетевого хранилища.

Чтобы осуществлять работу с сетевым хранилищем, необходимо подключить Kaspersky Security для Windows Server к защищаемому хранилищу в качестве *внешнего модуля*. Подключение подразумевает получение уведомлений о файловых операциях, выполняемых внешним модулем в защищаемом сетевом хранилище, анализ шаблонов полученных файловых операций, отправление заключений о файловой активности (можно ли ее оценить как попытку шифрования) и блокировка скомпрометированных узлов. Чтобы запустить задачу Защита от шифрования для NetApp, сервер (с установленной программой Kaspersky Security для Windows Server) должен быть указан как основной сервер FPolicy на стороне сетевого хранилища. FPolicy – это система уведомлений о доступе к файлам, которая нужна для отслеживания и управления событиями доступа к файлам в виртуальной системе хранения данных (Storage Virtual Machine, SVM) с томами FlexVol. Система создает уведомления, рассылаемые на внешние серверы FPolicy.

**FPolicy не поддерживает тома FlexGroup, поэтому компонент Защита от шифрования для NetApp нельзя настроить для защиты сетевых хранилищ с томами FlexGroup.**

Уведомления от сетевого хранилища передаются на внешний сервер по протоколу FPolicy только в синхронном режиме. Сервер анализирует каждое уведомление, прежде чем разрешить файловую операцию.

Связь между внешним модулем (Kaspersky Security для Windows Server) и защищаемым сетевым хранилищем осуществляется по протоколу FPolicy.

Чтобы настроить защиту, выполните следующие действия:

1. Создайте и настройте FPolicy на стороне защищаемого сетевого хранилища.
2. Укажите Kaspersky Security для Windows Server как сервер FPolicy на стороне защищаемого сетевого хранилища. Kaspersky Security для Windows Server будет распознаваться как внешний сервер.
3. Настройте параметры задачи Защита от шифрования для NetApp в Kaspersky Security для Windows Server.

Чтобы выполнить необходимую настройку, вам потребуются следующие данные:

- Имя машины SVM.
- IP-адрес и имя внешнего сервера.
- Полный список узлов кластеров защищаемых сетевых хранилищ, а также их имена.
- Адрес интерфейса управления кластером.
- Имя созданного протокола FPolicy.
- Порт для установки безопасного соединения между защищаемым сетевым хранилищем и внешним сервером.
- Учетные данные (имя и пароль):
  - для пользователя, которому разрешен доступ к общим папкам в сетевом хранилище;



- для локального администратора CDOT.

Эти параметры потребуется указать во время создания FPolicy (см. раздел "Создание и настройка FPolicy" на стр. 649) и настройки задачи Защита от шифрования для NetApp в Kaspersky Security для Windows Server (см. раздел "Настройка параметров задачи Защита от шифрования для NetApp" на стр. 655).

Подробные инструкции по созданию FPolicy см. в следующей статье <https://library.netapp.com/ecmdocs/ECMP12454941/html/GUID-DDFB957B-CE0F-4603-9629-669653B1E922.html>.

## Создание и настройка FPolicy

При первом создании FPolicy специалисты "Лаборатории Касперского" рекомендуют применять настройки, указанные в таблице ниже.

Table 93. Параметры FPolicy

| Параметр                                                                                                                                                                                                                               | Строка                                | Значение                                                                                                      | Примечание                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>_EVENT CREATE</b><br><br>Этот параметр определяет файловые операции, которые будут перехватываться и о которых будут отправляться уведомления в Kaspersky Security для Windows Server для анализа и обнаружения попыток шифрования. | <b>Имя сервера Vserver</b>            | <имя_svm>                                                                                                     | Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля (Kaspersky Security для Windows Server). |
|                                                                                                                                                                                                                                        | <b>Событие</b>                        | <источник_событий>                                                                                            | Будет использоваться как источник для FPolicy.                                                                                                                            |
|                                                                                                                                                                                                                                        | <b>Протокол</b>                       | cifs                                                                                                          |                                                                                                                                                                           |
|                                                                                                                                                                                                                                        | <b>Файловые операции</b>              | create, open, rename, write, close, setattr, delete                                                           |                                                                                                                                                                           |
|                                                                                                                                                                                                                                        | <b>Фильтры</b>                        | close-with-modification, first-write, write-with-size-change, open-with-delete-intent, open-with-write-intent |                                                                                                                                                                           |
|                                                                                                                                                                                                                                        | <b>Требуются ли дисковые операции</b> | false                                                                                                         |                                                                                                                                                                           |

|                                                                                                                             |                                        |                                     |                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>_ENGINE CREATE</b></p> <p>Этот параметр определяет параметры подключения к внешнему модулю (или серверу FPolicy).</p> | <b>Имя сервера Vserver</b>             | <имя_svm>                           | Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.                                      |
|                                                                                                                             | <b>Модуль</b>                          | <имя_модуля>                        | Имя внешнего модуля. Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.                 |
|                                                                                                                             | <b>Основные серверы FPolicy</b>        | <ip-адрес_основного_сервера>        | Можно указать только один сервер.                                                                                                                                      |
|                                                                                                                             | <b>Номер порта службы FPolicy</b>      | <номер_порта>                       | Рекомендуется указать значение 1346. Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля. |
|                                                                                                                             | <b>Вспомогательные серверы FPolicy</b> | <ip-адрес_вспомогательного_сервера> | Если выбран основной сервер, вспомогательный сервер недоступен.                                                                                                        |
|                                                                                                                             | <b>Тип внешнего модуля</b>             | Синхронный                          | Асинхронный режим не поддерживается.                                                                                                                                   |

|                                                                                     |                                            |                    |                                                                                                                                                                  |
|-------------------------------------------------------------------------------------|--------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                     | <b>Вариант SSL для внешнего соединения</b> | No-auth            |                                                                                                                                                                  |
|                                                                                     | <b>FQDN или CCN</b>                        | -                  |                                                                                                                                                                  |
|                                                                                     | <b>Серийный номер сертификата</b>          | -                  |                                                                                                                                                                  |
|                                                                                     | <b>Центр сертификации</b>                  | -                  |                                                                                                                                                                  |
| <b>_POLICY CREATE</b><br><br>Этот параметр определяет будущую конфигурацию FPolicy. | <b>Имя сервера Vserver</b>                 | <имя_svm>          | Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.                                |
|                                                                                     | <b>Fpolicy</b>                             | <имя_fpolicy>      | Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля.                                |
|                                                                                     | <b>Отслеживаемые события</b>               | <источник_событий> |                                                                                                                                                                  |
|                                                                                     | <b>Модуль FPolicy</b>                      | <имя_модуля>       | Строковое имя внешнего модуля. Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp на стороне внешнего модуля. |
|                                                                                     | <b>Требуется ли обязательная проверка</b>  | true               |                                                                                                                                                                  |

|                                                                                                  |                                                        |                    |                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                  | <b>Разрешить привилегированный доступ</b>              | yes                |                                                                                                                                                                             |
|                                                                                                  | <b>Имя пользователя для привилегированного доступа</b> | <имя_пользователя> | Значение должно совпадать со значением, указанным в параметрах задачи Защита от шифрования для NetApp в поле Учетные данные для доступа к общим папкам в сетевом хранилище. |
|                                                                                                  | <b>Включено ли транзитное чтение</b>                   | false              |                                                                                                                                                                             |
| SCOPE CREATE<br><br>Этот параметр определяет область защиты, за которую отвечает внешний модуль. | <b>Имя сервера Vserver</b>                             | <имя_svm>          | Рекомендуется указать максимально возможную область для защиты сетевых хранилищ. Рекомендуется добавить исключения в параметрах задачи Защита от шифрования для NetApp.     |
|                                                                                                  | <b>Политика</b>                                        | <имя_fpolicy>      |                                                                                                                                                                             |

Рекомендуется указать в таблице максимально возможные значения. Прочие значения могут варьироваться в зависимости от ваших требований.

При изменении параметров FPolicy на сетевом хранилище во время работы задачи Защита от шифрования для NetApp, необходимо перезапустить эту задачу, чтобы изменения вступили в силу.

## Настройка Kaspersky Security для Windows Server

Чтобы установить соединение между компонентом Защита от шифрования для NetApp (в Kaspersky Security для Windows Server) и защищаемым сетевым хранилищем, необходимо настроить параметры задачи Защита от шифрования для NetApp (см. таблицу ниже).

Table 94. Параметры задачи Защита от шифрования

| Параметр                        | Возможные значения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | По умолчанию                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>Режим</b>                    | <ul style="list-style-type: none"> <li>Только сообщать</li> <li>Активный</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Активный                             |
| <b>Эвристический анализатор</b> | Поверхностный – Средний – Глубокий                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Применяется Средний уровень анализа. |
| <b>Исключения</b>               | Применяется для всех защищаемых ресурсов общего доступа.<br>Критерии исключений: <ul style="list-style-type: none"> <li>Маска (папка, объект, расширение)</li> <li>IP-адрес клиентского компьютера</li> <li>Доверенный пользователь</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                | Не задано                            |
| <b>Адресация</b>                | <ul style="list-style-type: none"> <li>IP-адрес кластера</li> <li>Полный список кластеров</li> <li>Учетные данные (имя и пароль) для локального администратора CDOT.</li> </ul> Следующий параметр дублирует значение, установленное для параметра _POLICY CREATE (строка с именем пользователя для привилегированного доступа)<br>Учетные данные (имя и пароль) пользователя, которому разрешен доступ к папкам общего доступа в сетевом хранилище.<br>Следующие параметры дублируют значения, установленные для параметра _ENGINE CREATE в сетевом хранилище. <ul style="list-style-type: none"> <li>Имя FPolicy</li> <li>Имя SVM (Vserver)</li> <li>Порт (1346)</li> </ul> | Не задано                            |
| <b>Параметры расписания</b>     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Не задано                            |

### Использование Хранилища заблокированных узлов

Хранилище заблокированных узлов пополняется при выполнении следующих условий:

- Задача Защита от шифрования для NetApp запущена в режиме **Активный**.
- Защита от шифрования для NetApp определяет попытки шифрования защищаемых ресурсов общего доступа NetApp.

После обнаружения попытки шифрования компонент Защита от шифрования для NetApp отправляет информацию о скомпрометированном узле в **Хранилище заблокированных узлов**. После этого Kaspersky Security для Windows Server создает критическое событие блокировки узла и блокирует все файловые операции со стороны этого узла.

По умолчанию Kaspersky Security для Windows Server автоматически разблокирует узлы через 30 минут после их добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка недоверенных.

Список заблокированных узлов можно изменять следующими способами:

- разблокировать узлы вручную;
- настраивать длительность блокировки.

При настройке задачи Защита от шифрования для NetApp обратите внимание на тип внешнего модуля, используемого в параметрах FPolicy (параметр `_ENGINE CREATE`).

Kaspersky Security для Windows Server регистрирует событие с результатом полученного заключения и выполняет действия в соответствии с режимом работы.

Kaspersky Security для Windows Server поддерживает две возможные конфигурации:

| # | Режим работы сетевого хранилища | Режим работы задачи Защита от шифрования для NetApp | Описание                                                                                                                                                                                                                                                                                      |
|---|---------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Синхронный                      | Только сообщать                                     | Эта конфигурация обеспечивает защиту от шифрования в режиме аудита: программа только регистрирует события шифрования. Вы можете перейти на конфигурацию 2 из Kaspersky Security для Windows Server.                                                                                           |
| 2 | Синхронный                      | Активный                                            | Эта конфигурация обеспечивает полную защиту: программа добавляет все скомпрометированные узлы в Хранилище заблокированных узлов и блокирует все файловые операции со стороны этих узлов. Вы можете перейти на конфигурацию 1 как из защищаемого сетевого хранилища, так и с внешнего сервера. |

Подробнее о том, как настроить Хранилище заблокированных узлов, см. в Руководстве администратора Kaspersky Security для Windows Server.

## Настройка параметров задачи Защита от шифрования для NetApp

Настройте параметры внешнего сервера и сетевого хранилища, чтобы запустить и настроить задачу Защита от шифрования для NetApp.

### В этом разделе

|                                                                                   |                     |
|-----------------------------------------------------------------------------------|---------------------|
| Настройка параметров задачи в Консоли Kaspersky Security для Windows Server ..... | <a href="#">655</a> |
| Настройка параметров задачи в Kaspersky Security Center .....                     | <a href="#">656</a> |
| Настройка общих параметров задачи .....                                           | <a href="#">656</a> |
| Настройка адресации .....                                                         | <a href="#">657</a> |
| Изменение списка исключений .....                                                 | <a href="#">658</a> |

## Настройка параметров задачи в Консоли Kaspersky Security для Windows Server

- Чтобы настроить задачу Защита от шифрования для NetApp, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита от шифрования для NetApp**.
3. В панели результатов перейдите по ссылке **Свойства**.  
Откроется окно **Параметры задачи**.
4. На закладке **Общие** настройте следующие параметры:
  - В разделе **Режим работы** выберите режим работы задачи.
  - В разделе **Эвристический анализатор** настройте использование эвристического анализатора и уровень эвристического анализа.
5. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. [657](#)).
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
7. Нажмите на кнопку **ОК**.

- Чтобы настроить список исключений для задачи Защита от шифрования для NetApp, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Защита сетевых хранилищ**.
2. Выберите вложенный узел **Защита от шифрования для NetApp**.
3. Перейдите по ссылке **Список исключений** в панели результатов.  
Откроется окно **Список исключений**.
4. Настройте список исключений (см. раздел "Изменение списка исключений" на стр. [658](#)).

## Настройка параметров задачи в Kaspersky Security Center

► Чтобы настроить задачу *Защита от шифрования для NetApp*, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. Чтобы настроить параметры программы для группы серверов, выберите закладку **Политики** и откройте свойства политики, которую вы хотите изменить.
3. В разделе **Защита сетевых хранилищ** в блоке **Защита от шифрования для NetApp** нажмите на кнопку **Настройка**.
4. На закладке **Общие** настройте режим работы задачи и эвристический анализатор.
5. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. [657](#)).
6. На закладке **Исключения** добавьте исключения из области защиты (см. раздел "Изменение списка исключений" на стр. [658](#)).
7. На закладке **Управление задачами** настройте запуск задачи по расписанию.
8. Нажмите на кнопку **ОК**.

## Настройка общих параметров задачи

► Чтобы настроить задачу *Защита от шифрования для NetApp*, выполните следующие действия:

1. На закладке **Общие** настройте следующие параметры:
  - **Режим работы задачи:**
    - **Только сообщать**

Выберите этот вариант, чтобы получать уведомления об обнаруженных попытках шифрования файлов. Программа создает события в журнале выполнения задачи.
    - **Активный**

Выберите этот вариант, чтобы блокировать файловые операции, выполняемые скомпрометированными узлами в сетевом хранилище. При обнаружении попытки шифрования файлов программа добавляет узлы в Хранилище заблокированных узлов. Все файловые операции с этого компьютера будут заблокированы на период, указанный в параметрах хранилища.
  - **Эвристический анализатор:**
    - Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора при проверке объектов.

Если флажок установлен, эвристический анализатор включен.



Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

- Если требуется, отрегулируйте уровень анализа с помощью ползунка.

Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

Этот уровень выбран по умолчанию.

- **Глубокий.** Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

2. На закладке **Адресация** настройте параметры соединения и аутентификации (см. раздел "Настройка адресации" на стр. [657](#)).
3. На закладке **Исключения** добавьте исключения из области защиты (см. раздел "Изменение списка исключений" на стр. [658](#)).
4. На закладке **Управление задачами** настройте запуск задачи по расписанию.
5. Нажмите на кнопку **ОК**.

## Настройка адресации

- Чтобы настроить соединение с защищаемыми кластерами и получить доступ к сетевому хранилищу, выполните следующие действия:

1. В параметрах задачи откройте закладку **Адресация**.
2. В разделе **Соединение** настройте следующие параметры:

- **IP-адрес защищаемого кластера**

Укажите IP-адрес кластера. Кластер содержит следующие типы серверов Vserver:

- сервер администрирования Vserver;
- узел Vserver;
- кластер Vserver.

- **Имя сервера Vserver**

Укажите имя виртуального сервера хранения.

- **Имя FPolicy**

Укажите имя FPolicy. Прежде чем FPolicy сможет проверять доступ к файлам, требуется создать конфигурацию FPolicy и включить ее на сервере Vserver, для которого нужны службы FPolicy.

- **Порт**

3. Чтобы изменить список защищаемых узлов кластера, выполните следующие действия:

- a. В разделе **Соединение** выберите **Список узлов кластера**.
- b. Введите имя узла.
- c. Нажмите на кнопку **Добавить**.
- d. Нажмите на кнопку **ОК**.

Все существующие узлы защищаемого кластера необходимо добавить в список.

4. В разделе **Аутентификация** укажите следующие данные:

- Учетные данные пользователя с привилегированным доступом к папкам сетевого хранилища: имя и пароль.

Эти учетные данные должны совпадать с данными, указанными при выполнении команды `_POLICY CREATE` на стороне сетевого хранилища.

- Учетные данные администратора CDOT: имя и пароль.

5. В окне **Защита от шифрования для NetApp** нажмите на кнопку **ОК**.

Настроенные параметры адресации будут сохранены.

## Изменение списка исключений

Можно добавлять исключения на основе следующих критериев:

- путь;
- IP-адрес;
- идентификатор пользователя.

Для исключений можно использовать любые сочетания этих критериев. Чем больше критериев вы укажете, тем строже будут параметры исключения. Kaspersky Security для Windows Server не анализирует файловые операции для указанных исключений. Обратите внимание, что добавленные в этот список исключения используются для всех папок в сетевом хранилище.

Если вы одновременно настраиваете антивирусную защиту и FPolicy для одного сетевого хранилища, доступ к общим сетевым папкам хранилища будет возможен только при запущенных задачах **Защита RPC-подключаемых сетевых хранилищ** и **Защита от шифрования для NetApp**.

Внешний модуль должен иметь только одну сетевую плату с одним IP-адресом.

► Чтобы добавить или изменить список исключений, выполните следующие действия:

1. В параметрах задачи откройте закладку **Исключения**.
2. Установите флажок **Не обнаруживать шифрование для указанных исключений**.

Если флажок установлен, разрешены все файловые операции, выполняемые указанным в списке ниже пользователем, с указанного IP-адреса или по указанному пути.

Если флажок снят, Kaspersky Security для Windows Server обнаруживает активность шифрования со стороны всех пользователей и узлов и со всех путей.

По умолчанию флажок снят.

Список исключений будет активирован.

3. Нажмите на кнопку **Добавить**.  
Откроется окно **Параметры исключений**.
4. Чтобы добавить исключение по маске, выполните следующие действия:
  - a. На закладке **Путь** установите флажок **Исключать по маске пути**.
  - b. Укажите путь.
  - c. Нажмите на кнопку **Добавить**.
5. Чтобы добавить исключение на основе IP-адреса, выполните следующие действия:
  - a. На закладке **IP-адреса** установите флажок **Исключать по IP-адресу клиентского компьютера**.
  - b. Введите IP-адрес.
  - c. Нажмите на кнопку **Добавить**.
6. Чтобы добавить исключение на основе имени пользователя, выполните следующие действия:
  - a. На закладке **Пользователи** установите флажок **Исключать по имени пользователя**.
  - b. Нажмите на кнопку **Добавить**.  
Откроется окно **Выбор пользователей**.
  - c. Выберите пользователя или группу, которую вы хотите исключить.
  - d. Нажмите на кнопку **ОК**.
7. В окне **Параметры исключений** нажмите на кнопку **ОК**.  
Список исключений пополнится указанными исключениями.

## Управление задачами защиты сетевых хранилищ из Kaspersky Security Center

В этом разделе приведена информация об управлении задачами защиты сетевых хранилищ с помощью Сервера администрирования Kaspersky Security Center, а также инструкции по настройке параметров задач для группы серверов и для одного сервера из Kaspersky Security Center.

Вы можете управлять задачами защиты сетевых хранилищ из Kaspersky Security Center следующими способами:

- С помощью политик Kaspersky Security Center. Вы можете настроить единые параметры защиты сетевых хранилищ и применить их в задачах выбранной группы серверов.
- В окне **Свойства устройства**. Вы можете настроить параметры защиты сетевых хранилищ отдельно для каждого сервера, на котором установлена программа Kaspersky Security для Windows Server.

### В этом разделе

|                                                                                                           |                     |
|-----------------------------------------------------------------------------------------------------------|---------------------|
| Настройка параметров защиты сетевых хранилищ с помощью политик .....                                      | <a href="#">660</a> |
| Настройка параметров защиты сетевых хранилищ для одного сервера в Kaspersky Security Center .....         | <a href="#">662</a> |
| Настройка параметров уровня безопасности вручную в задаче Защита RPC-подключаемых сетевых хранилищ .....  | <a href="#">663</a> |
| Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ ..... | <a href="#">666</a> |

## Настройка параметров защиты сетевых хранилищ с помощью политик

По умолчанию в задачах защиты сетевых хранилищ в политике Kaspersky Security Center используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Table 95. Параметры задач защиты сетевых хранилищ в политиках Kaspersky Security Center

| Задача защиты сетевых хранилищ                  | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Защита RPC-подключаемых сетевых хранилищ</b> | <p>В разделе <b>Защита RPC-подключаемых сетевых хранилищ</b> по кнопке <b>Настройка</b> можно настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>• указать область защиты;</li> <li>• задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;</li> <li>• настроить использование эвристического анализатора;</li> <li>• настроить применение доверенной зоны и использование KSN;</li> </ul> |

| Задача защиты сетевых хранилищ                   | Параметры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | <ul style="list-style-type: none"> <li>настроить параметры соединения с сетевым хранилищем;</li> <li>настроить параметры запуска задачи.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Защита ICAP-подключаемых сетевых хранилищ</b> | <p>В разделе <b>Защита ICAP-подключаемых сетевых хранилищ</b> по кнопке <b>Настройка</b> можно настроить следующие параметры задачи:</p> <ul style="list-style-type: none"> <li>настроить использование эвристического анализатора;</li> <li>настроить параметры соединения с сетевым хранилищем;</li> <li>задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;</li> <li>настроить использование KSN;</li> <li>настроить параметры запуска задачи.</li> </ul> |
| <b>Защита от шифрования для NetApp</b>           | <p>В разделе <b>Защита от шифрования для NetApp</b> по кнопке <b>Настройка</b> можно настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>режим работы задачи;</li> <li>использование эвристического анализатора;</li> <li>параметры подключения и аутентификации;</li> <li>исключения из области защиты.</li> </ul>                                                                                                                                                                                                                           |

► Чтобы настроить параметры задач защиты сетевых хранилищ в политике Kaspersky Security Center, выполните следующие действия:

- В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
- В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Чтобы настроить параметры программы для группы серверов, выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:
    - Выберите пункт **Свойства** в контекстном меню политики.
    - Перейдите по ссылке **Настроить параметры политики** в панели результатов выбранной политики.
    - Двойным щелчком мыши по нужной политике.
- При настройке политики выберите пункт **Защита сетевых хранилищ** в списке разделов в окне **Свойства: <Имя политики>**.
- В открывшемся окне выполните следующие действия:
  - Чтобы настроить параметры задачи Защита RPC-подключаемых сетевых хранилищ, в разделе **Защита RPC-подключаемых сетевых хранилищ** нажмите на кнопку **Настройка**.  
В открывшемся окне параметров настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.
  - Чтобы настроить параметры задачи Защита ICAP-подключаемых сетевых хранилищ, в разделе **Защита ICAP-подключаемых сетевых хранилищ** нажмите на кнопку **Настройка**.

В открывшемся окне параметров настройте параметры задачи (см. раздел "Настройка параметров задачи Защита ICAP-подключаемых сетевых хранилищ" на стр. [636](#)) в соответствии с вашими требованиями. Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.

- Чтобы настроить параметры задачи Защита от шифрования для NetApp, в разделе **Защита от шифрования для NetApp** нажмите на кнопку **Настройка**.

В открывшемся окне параметров настройте параметры задачи (см. раздел "Настройка параметров задачи Защита от шифрования для NetApp" на стр. [655](#)) в соответствии с вашими требованиями. Нажмите на кнопку **ОК**, чтобы сохранить изменения параметров в политике.

5. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**.

Настроенные параметры задач защиты сетевых хранилищ будут сохранены и применены в активной политике.

Подробная информация о работе Kaspersky Security для Windows Server с политиками Kaspersky Security Center, а также информация о политиках Kaspersky Security Center приведена в *Руководстве администратора Kaspersky Security Center* и *Руководстве администратора Kaspersky Security для Windows Server*.

## Настройка параметров защиты сетевых хранилищ для одного сервера в Kaspersky Security Center

- Чтобы настроить параметры защиты сетевых хранилищ для одного сервера из Kaspersky Security Center, выполните следующие действия:

1. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый сервер.
2. В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом сервере и выберите пункт **Свойства**.
3. В окне **Свойства: <Имя компьютера>** в разделе **Задачи** откройте контекстное меню задачи защиты сетевых хранилищ, которую вы хотите настроить, и выберите пункт **Свойства**.
4. В открывшемся окне настройте параметры задачи защиты сетевых хранилищ в соответствии с вашими требованиями:
  - Задача Защита RPC-подключаемых сетевых хранилищ (см. раздел "Настройка параметров задачи Защита RPC-подключаемых сетевых хранилищ" на стр. [619](#)).
  - Задача Защита ICAP-подключаемых сетевых хранилищ.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены и применены к выполняющейся задаче на одном сервере.

Если к программе применяется политика Kaspersky Security Center и в этой политике запрещено изменение параметров задачи, эти параметры недоступны для изменения в окне **Свойства: <Имя компьютера>**.

Подробная информация о работе Kaspersky Security для Windows Server с политиками Kaspersky Security Center, а также информация о политиках Kaspersky Security Center приведена в *Руководстве администратора Kaspersky Security Center* и *Руководстве администратора Kaspersky Security для Windows Server*.

## Настройка параметров уровня безопасности вручную в задаче **Защита RPC-подключаемых сетевых хранилищ**

- Чтобы вручную настроить параметры безопасности для RPC-подключаемого сетевого хранилища, выполните следующие действия:
1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
  2. Выберите группу администрирования, для которой вы хотите настроить задачу.
  3. Выберите закладку **Политики**.
  4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
  5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Защита сетевых хранилищ**.
  6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов (RPC)**.  
Откроется окно **Защита RPC-подключаемых сетевых хранилищ**.
  7. Выберите закладку **Область защиты**.
  8. Чтобы добавить, изменить или удалить сетевое хранилище, выполните следующие действия:
    - Нажмите на кнопку **Добавить**, чтобы добавить RPC-подключаемое сетевое хранилище в область защиты Kaspersky Security для Windows Server.
    - В списке защищаемых сетевых хранилищ выберите сетевое хранилище и нажмите на кнопку **Изменить**, чтобы изменить сетевое хранилище.
    - В списке защищаемых сетевых хранилищ выберите сетевое хранилище и нажмите на кнопку **Удалить**, чтобы удалить сетевое хранилище.
  9. В списке защищаемых сетевых хранилищ выберите сетевое хранилище и нажмите на кнопку **Настроить**.  
Откроется окно **Настройка защиты RPC-подключаемых сетевых хранилищ**.

Вы можете применить предварительно созданный шаблон параметров безопасности.

10. Нажмите на кнопку **Настройка**.

11. Настройте параметры для выбранного сетевого хранилища в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:

- На закладке **Общие** выполните следующие действия:
  - В разделе **Защита объектов** укажите объекты, которые будет проверять Kaspersky Security для Windows Server:
    - **Все объекты**  
Kaspersky Security для Windows Server проверяет все объекты.
    - **Объекты, проверяемые по формату**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.  
Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
    - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.  
Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
    - **Объекты, проверяемые по указанному списку расширений**  
Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

Этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.

- В разделе **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security для Windows Server.
- На закладке **Действия** выполните следующие действия:
  - В разделе **Действия над зараженными и другими обнаруженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении зараженного объекта.



- В разделе **Действия над возможно зараженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении возможно зараженного объекта.
- Настройте действия над объектами в зависимости от типа обнаруженного объекта.
- Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

Флажок включает или выключает принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Security для Windows Server не выполняет выбранное действие, если родительский объект неизменяем.

- На закладке **Производительность** выполните следующие действия:
  - В разделе **Исключения** укажите, какие объекты Kaspersky Security для Windows Server исключает из проверки:
    - Чтобы исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
    - Чтобы исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии <http://www.securelist.ru>.
  - В разделе **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.

Если вы используете сетевое хранилище, работающее под управлением операционной системы Clustered Data ONTAP, этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.

12. Нажмите на кнопку **ОК**.

Настроенные параметры пользовательского уровня безопасности будут сохранены и применены в выполняющейся задаче.

## Настройка параметров уровня безопасности вручную в задаче Защита ICAP-подключаемых сетевых хранилищ

По умолчанию в задаче Защита ICAP-подключаемых сетевых хранилищ используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

При изменении параметров задачи, например, выборе другого уровня безопасности, Kaspersky Security для Windows Server немедленно применит новые значения параметров в выполняющейся задаче. Kaspersky Security для Windows Server сохранит в журнале системного аудита дату и время изменения параметров задачи.

Table 96. Параметры задачи Защита ICAP-подключаемых сетевых хранилищ

| Параметр                                  | Значение по умолчанию                                                                                                                | Комментарий                                                                                                                                            |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Уровень безопасности                      | Применяется уровень безопасности <b>Рекомендуемый</b> .                                                                              | Вы можете применить к защищаемому сетевому хранилищу один из стандартных уровней безопасности, или настроить значения параметров безопасности вручную. |
| Эвристический анализатор                  | Применяется уровень анализа <b>Средний</b> .                                                                                         | Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.                                                    |
| Использование KSN для защиты              | Применяется.                                                                                                                         | Вы можете включать и выключать использование служб KSN для защиты ICAP-подключаемых сетевых хранилищ.                                                  |
| Параметры соединения с сетевым хранилищем | <ul style="list-style-type: none"> <li><b>Номер сетевого порта</b> – 1344.</li> <li><b>Идентификатор службы</b> – avscan.</li> </ul> | Также можно изменить другие параметры соединения с сетевыми хранилищами. Эти изменения должны быть учтены на сетевых хранилищах.                       |
| Запуск задачи по расписанию               | Не применяется. Флажок <b>Запускать задачу по расписанию</b> снят. Задача запускается вручную.                                       | Вы можете настроить запуск задачи по расписанию, например, при запуске Kaspersky Security для Windows Server.                                          |

► Чтобы вручную настроить параметры безопасности для ICAP-подключаемого сетевого хранилища, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Защита сетевых хранилищ**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов (ICAP)**.

Откроется окно **Защита ICAP-подключаемых сетевых хранилищ**.

7. На закладке **Общие** окна **Защита ICAP-подключаемых сетевых хранилищ** нажмите на кнопку **Настройка**.

Откроется окно **Параметры безопасности**.

8. Настройте параметры в соответствии с вашими требованиями к компьютерной безопасности. Для этого выполните следующие действия:

- На закладке **Общие** выполните следующие действия:
  - В разделе **Защита объектов** укажите объекты, которые будет проверять Kaspersky Security для Windows Server:
    - **Все объекты**  
Kaspersky Security для Windows Server проверяет все объекты.
    - **Объекты, проверяемые по формату**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании формата файла.  
Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
    - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**  
Kaspersky Security для Windows Server проверяет только потенциально заражаемые файлы на основании расширения файла.  
Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Security для Windows Server.
    - **Объекты, проверяемые по указанному списку расширений**  
Kaspersky Security для Windows Server проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

Этот параметр можно также настроить в сетевом хранилище. Если параметр настроен в Kaspersky Security для Windows Server, то сетевое хранилище может отправить на проверку несоответствующий объект, а Kaspersky Security для Windows Server признает этот объект безопасным, не выполняя антивирусную проверку. Если параметр настроен в сетевом хранилище, то сетевое хранилище не отправляет на проверку несоответствующие объекты. В целях экономии сетевого трафика и снижения нагрузки на сервер с установленной программой Kaspersky Security для Windows Server, рекомендуется настраивать параметры, ограничивающие количество проверяемых объектов в сетевом хранилище.

- В разделе **Защита составных объектов** укажите, какие составные объекты проверяет Kaspersky Security для Windows Server.
- На закладке **Действия** выполните следующие действия:
  - В разделе **Действия над зараженными и другими обнаруженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении зараженного объекта.
  - В разделе **Действия над возможно зараженными объектами** выберите действие, которое Kaspersky Security для Windows Server выполняет при обнаружении возможно зараженного объекта.

- Настройте действия над объектами в зависимости от типа обнаруженного объекта.
- На закладке **Производительность** выполните следующие действия:
  - В разделе **Исключения** укажите, какие объекты Kaspersky Security для Windows Server исключает из проверки:
    - Чтобы исключить файлы из проверки, установите флажок **Исключать файлы** и укажите имена или маски имен файлов, которые нужно исключать.
    - Чтобы исключить обнаруживаемые объекты (например, утилиты удаленного администрирования), установите флажок **Не обнаруживать** и укажите имена или маски имен обнаруживаемых объектов согласно классификации Вирусной энциклопедии <http://www.securelist.ru>.
  - В разделе **Дополнительные параметры** укажите максимальную продолжительность проверки объекта и максимальный размер проверяемого составного файла.
- 9. В окне **Параметры безопасности** нажмите на кнопку **ОК**.

Окно **Параметры безопасности** закроется.
- 10. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры пользовательского уровня безопасности будут сохранены.

# Интеграция со сторонними системами

Этот раздел содержит описание интеграции Kaspersky Security для Windows Server с функциями и технологиями сторонних производителей.

## В этом разделе

|                                                                    |                     |
|--------------------------------------------------------------------|---------------------|
| Счетчики производительности для программы Системный монитор.....   | <a href="#">669</a> |
| Счетчики и ловушки SNMP Kaspersky Security для Windows Server..... | <a href="#">679</a> |
| Интеграция с WMI .....                                             | <a href="#">690</a> |

## Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы Системный монитор Microsoft Windows, которые регистрирует Kaspersky Security для Windows Server во время установки.

## В этом разделе

|                                                                              |                     |
|------------------------------------------------------------------------------|---------------------|
| О счетчиках производительности Kaspersky Security для Windows Server .....   | <a href="#">670</a> |
| Общее количество отвергнутых запросов .....                                  | <a href="#">671</a> |
| Общее количество пропущенных запросов .....                                  | <a href="#">672</a> |
| Количество запросов, не обработанных из-за нехватки системных ресурсов ..... | <a href="#">673</a> |
| Количество запросов, отправленных на обработку.....                          | <a href="#">674</a> |
| Среднее количество потоков диспетчера файловых перехватов.....               | <a href="#">675</a> |
| Максимальное количество потоков диспетчера файловых перехватов .....         | <a href="#">676</a> |
| Количество элементов в очереди зараженных объектов .....                     | <a href="#">677</a> |
| Количество объектов, обрабатываемых за секунду.....                          | <a href="#">678</a> |

## О счетчиках производительности Kaspersky Security для Windows Server

В состав устанавливаемых компонентов Kaspersky Security для Windows Server по умолчанию включен компонент Счетчики производительности. Во время установки Kaspersky Security для Windows Server регистрирует свои счетчики производительности для программы Системный монитор Microsoft Windows.

С помощью счетчиков Kaspersky Security для Windows Server вы можете контролировать производительность программы во время выполнения задач постоянной защиты сервера. Вы можете обнаружить узкие места и недостаточность ресурсов при совместной работе с другими программами. Вы можете диагностировать сбои в работе и неоптимальную настройку Kaspersky Security для Windows Server.

Вы можете просматривать счетчики производительности Kaspersky Security для Windows Server, открыв консоль **Производительность** Панели управления Windows в разделе **Администрирование**.

В следующих разделах приведены определения счетчиков, рекомендованные интервалы считывания показаний, пороговые значения и рекомендованные значения параметров Kaspersky Security для Windows Server для случаев, когда значения счетчиков превышают пороговые значения.

## Общее количество отвергнутых запросов

Table 97. Общее количество отвергнутых запросов

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                                                     | Общее количество отвергнутых запросов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Определение                                                  | <p>Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты процессами программы; рассчитывается с момента последнего запуска Kaspersky Security для Windows Server.</p> <p>Программа пропускает объекты, запросы на обработку которых отвергаются процессами Kaspersky Security для Windows Server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Назначение                                                   | <p>Счетчик позволяет обнаруживать следующие ситуации:</p> <ul style="list-style-type: none"> <li>снижение эффективности постоянной защиты сервера из-за повышенной нагрузки на процессы Kaspersky Security для Windows Server;</li> <li>прерывание постоянной защиты сервера из-за отказа диспетчера файловых перехватов.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Нормальное / пороговое значение                              | 0 / 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Рекомендуемый интервал считывания показаний                  | 1 час                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Рекомендации по настройке, если значение превышает пороговое | <p>Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов.</p> <p>Возможны следующие ситуации в зависимости от поведения счетчика:</p> <ul style="list-style-type: none"> <li>Счетчик показывает несколько запросов, отвергнутых в течение длительного времени: все процессы Kaspersky Security для Windows Server были полностью загружены, поэтому программа Kaspersky Security для Windows Server не смогла проверить объекты.</li> </ul> <p>Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты сервера. Можно использовать такие параметры Kaspersky Security для Windows Server, как <b>Максимальное количество активных процессов</b> и <b>Количество процессов для постоянной защиты</b>.</p> <ul style="list-style-type: none"> <li>Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Security для Windows Server не проверяет объекты при обращении к ним.</li> </ul> <p>Перезапустите Kaspersky Security для Windows Server.</p> |

## Общее количество пропущенных запросов

Table 98. Общее количество пропущенных запросов

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                                                     | Общее количество пропущенных запросов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Определение                                                  | <p>Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Security для Windows Server, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы.</p> <p>Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика <b>Общее количество пропущенных запросов</b> увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Security для Windows Server пропускает такой объект и значение счетчика <b>Общее количество пропущенных запросов</b> увеличивается на 1.</p> |
| Назначение                                                   | Счетчик позволяет обнаруживать снижение производительности из-за сбоев диспетчера файловых перехватов.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Нормальное / пороговое значение                              | 0 / 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Рекомендуемый интервал считывания показаний                  | 1 час                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Рекомендации по настройке, если значение превышает пороговое | <p>Если значение счетчика отличается от нуля, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент.</p> <p>Если скорость проверки не удовлетворительна, перезапустите Kaspersky Security для Windows Server, чтобы восстановить простаивающие потоки.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |



## Количество запросов, не обработанных из-за нехватки системных ресурсов

Table 99. Количество запросов, не обработанных из-за нехватки системных ресурсов

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Количество запросов, не обработанных из-за нехватки системных ресурсов<br>(Number of requests not processed due to lack of resources)                                                                                                                                                                                                                                    |
| <b>Определение</b>                                                  | Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Security для Windows Server.<br>Kaspersky Security для Windows Server пропускает запросы на обработку объектов, которые не обрабатываются драйвером файловых перехватов. |
| <b>Назначение</b>                                                   | Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты сервера, возникающее из-за недостаточности системных ресурсов.                                                                                                                                                                                                                  |
| <b>Нормальное / пороговое значение</b>                              | 0 / 1                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 час                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | Если значение счетчика отличается от нуля, рабочим процессам Kaspersky Security для Windows Server требуется больший объем оперативной памяти для обработки запросов.<br>Возможно, активные процессы других программ используют всю доступную оперативную память.                                                                                                        |

## Количество запросов, отправленных на обработку

Table 100. Количество запросов, отправленных на обработку

|                                                                     |                                                                                                                                                              |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Количество запросов, отправленных на обработку.                                                                                                              |
| <b>Определение</b>                                                  | Количество объектов, ожидающих обработки рабочими процессами.                                                                                                |
| <b>Назначение</b>                                                   | Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Security для Windows Server и общий уровень файловой активности на защищаемом устройстве. |
| <b>Нормальное / пороговое значение</b>                              | Значение счетчика может изменяться в зависимости от уровня файловой активности на защищаемом устройстве.                                                     |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 мин.                                                                                                                                                       |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | Недоступно                                                                                                                                                   |

## Среднее количество потоков диспетчера файловых перехватов

Table 101. Среднее количество потоков диспетчера файловых перехватов

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Определение</b>                                                  | Количество потоков диспетчера файловых перехватов в одном процессе и среднее по всем процессам, участвующим в задачах постоянной защиты сервера.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Назначение</b>                                                   | Счетчик позволяет обнаруживать и устранять возможное снижение уровня постоянной защиты сервера из-за полной загрузки процессов Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Нормальное / пороговое значение</b>                              | Варьируется / 40.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 мин.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | <p>В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Kaspersky Security для Windows Server пропустит объект.</p> <p>Увеличьте количество процессов Kaspersky Security для Windows Server для задач постоянной защиты сервера. Можно использовать такие параметры Kaspersky Security для Windows Server, как <b>Максимальное количество активных процессов</b> и <b>Количество процессов для постоянной защиты</b>.</p> |

## Максимальное количество потоков диспетчера файловых перехватов

Table 102. Максимальное количество потоков диспетчера файловых перехватов

|                                                                     |                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).                                                                                                                                                                                             |
| <b>Определение</b>                                                  | Количество потоков диспетчера файловых перехватов в одном процессе и максимальное по всем процессам, участвующим в задачах постоянной защиты сервера.                                                                                                                                                                |
| <b>Назначение</b>                                                   | Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.                                                                                                                                                                |
| <b>Нормальное / пороговое значение</b>                              | Варьируется / 40.                                                                                                                                                                                                                                                                                                    |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 мин.                                                                                                                                                                                                                                                                                                               |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | Если значение этого счетчика значительно и продолжительно превышает значение счетчика <b>Среднее количество потоков диспетчера файловых перехватов</b> , Kaspersky Security для Windows Server неравномерно распределяет нагрузку на выполняющиеся процессы.<br>Перезапустите Kaspersky Security для Windows Server. |

## Количество элементов в очереди зараженных объектов

Table 103. Количество элементов в очереди зараженных объектов

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Количество элементов в очереди зараженных объектов.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Определение</b>                                                  | Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Назначение</b>                                                   | <p>Счетчик позволяет обнаруживать следующие ситуации:</p> <ul style="list-style-type: none"> <li>• прерывание постоянной защиты сервера из-за возможного отказа диспетчера файловых перехватов;</li> <li>• перегруженность процессов из-за неравномерного распределения процессорного времени между рабочими процессами и Kaspersky Security для Windows Server;</li> <li>• вирусную эпидемию.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Нормальное / пороговое значение</b>                              | Значение счетчика может быть отличным от нуля, пока Kaspersky Security для Windows Server обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 мин.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | <p>Если значение счетчика остается ненулевым длительное время:</p> <ul style="list-style-type: none"> <li>• Kaspersky Security для Windows Server не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов).<br/>Перезапустите Kaspersky Security для Windows Server.</li> <li>• Не хватает процессорного времени для обработки объектов.<br/>Обеспечьте выделение Kaspersky Security для Windows Server дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ.</li> <li>• Возникла вирусная эпидемия.</li> </ul> <p>О возникновении вирусной эпидемии свидетельствует большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи.</p> |

## Количество объектов, обрабатываемых за секунду

Table 104. Количество объектов, обрабатываемых за секунду

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Название</b>                                                     | Количество объектов, обрабатываемых за секунду (Number of objects processed per second)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Определение</b>                                                  | Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Назначение</b>                                                   | Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности защищаемого устройства, возникшее из-за недостаточности процессорного времени, выделяемого рабочим процессам Kaspersky Security для Windows Server, или сбоев в работе Kaspersky Security для Windows Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Нормальное / пороговое значение</b>                              | Варьируется / Нет.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Рекомендуемый интервал считывания показаний</b>                  | 1 мин.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Рекомендации по настройке, если значение превышает пороговое</b> | <p>Значения счетчика зависят от установленных значений параметров Kaspersky Security для Windows Server и загрузки защищаемого устройства процессами других программ.</p> <p>Отслеживайте среднее значение показаний счетчика в течение продолжительного времени. Если среднее значение показаний счетчика снизилось, то могла возникнуть одна из следующих ситуаций:</p> <ul style="list-style-type: none"> <li>• Рабочим процессам Kaspersky Security для Windows Server не хватает процессорного времени для обработки объектов.</li> </ul> <p>Обеспечьте выделение Kaspersky Security для Windows Server дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ.</p> <ul style="list-style-type: none"> <li>• Возник сбой в работе Kaspersky Security для Windows Server (простаивает несколько потоков).</li> </ul> <p>Перезапустите Kaspersky Security для Windows Server.</p> |

## Счетчики и ловушки SNMP Kaspersky Security для Windows Server

Этот раздел содержит информацию о счетчиках и ловушках Kaspersky Security для Windows Server.

### В этом разделе

|                                                                                                   |                     |
|---------------------------------------------------------------------------------------------------|---------------------|
| О счетчиках и ловушках SNMP Kaspersky Security для Windows Server .....                           | <a href="#">679</a> |
| SNMP-счетчики Kaspersky Security для Windows Server .....                                         | <a href="#">679</a> |
| SNMP-ловушки Kaspersky Security для Windows Server и их параметры.....                            | <a href="#">683</a> |
| Описания и возможные значения параметров SNMP-ловушек Kaspersky Security для Windows Server ..... | <a href="#">687</a> |

## О счетчиках и ловушках SNMP Kaspersky Security для Windows Server

Если вы включили компонент Счетчики и ловушки SNMP в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Security для Windows Server по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Security для Windows Server на рабочем месте администратора, запустите на защищаемом устройстве Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

## SNMP-счетчики Kaspersky Security для Windows Server

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Security для Windows Server.

### В этом разделе

|                                         |                     |
|-----------------------------------------|---------------------|
| Счетчики производительности .....       | <a href="#">680</a> |
| Счетчики карантина .....                | <a href="#">680</a> |
| Счетчик резервного хранилища .....      | <a href="#">680</a> |
| Общие счетчики .....                    | <a href="#">681</a> |
| Счетчик обновлений .....                | <a href="#">681</a> |
| Счетчики постоянной защиты файлов ..... | <a href="#">682</a> |
| Счетчики Проверки скриптов .....        | <a href="#">683</a> |
| Счетчики Защиты трафика.....            | <a href="#">683</a> |

## Счетчики производительности

Table 105. *Счетчики производительности*

| Счетчик                     | Определение                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------|
| currentRequestsAmount       | Количество запросов, отправленных на обработку (см. стр. <a href="#">674</a> )      |
| currentInfectedQueueLength  | Количество элементов в очереди зараженных объектов (см. стр. <a href="#">677</a> )  |
| currentObjectProcessingRate | Количество объектов, обрабатываемых за секунду (см. стр. <a href="#">678</a> )      |
| currentWorkProcessesNumber  | Количество рабочих процессов Kaspersky Security для Windows Server в текущий момент |

## Счетчики карантина

Table 106. *Счетчики карантина*

| Счетчик                | Определение                                                                |
|------------------------|----------------------------------------------------------------------------|
| totalObjects           | Количество объектов в папке карантина в текущий момент                     |
| totalSuspiciousObjects | Количество возможно зараженных объектов в папке карантина в текущий момент |
| currentStorageSize     | Общий объем данных в папке карантина (МБ)                                  |

## Счетчик резервного хранилища

Table 107. *Счетчик резервного хранилища*

| Счетчик                  | Определение                                          |
|--------------------------|------------------------------------------------------|
| currentBackupStorageSize | Общий объем данных в папке резервного хранилища (МБ) |



## Общие счетчики

Table 108. Общие счетчики

| Счетчик                            | Определение                                                                                                                                                                        |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lastCriticalAreasScanAge           | Период с момента проведения последней полной проверки важных областей защищаемого устройства (промежуток времени в секундах с момента завершения задачи Проверка важных областей). |
| licenseExpirationDate              | Дата окончания срока действия лицензии. Если добавлен активный и дополнительный ключ, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом.      |
| currentApplicationUptime           | Время работы Kaspersky Security для Windows Server с момента его последнего запуска, в сотых долях секунды                                                                         |
| currentFileMonitorTaskStatus       | Статус задачи Постоянная защита файлов: <b>Вкл.</b> – запущена; <b>Выкл.</b> – остановлена или приостановлена.                                                                     |
| currentScriptCheckerTaskStatus     | Статус задачи Проверка скриптов: <b>Вкл.</b> – запущена; <b>Выкл.</b> – остановлена или приостановлена.                                                                            |
| currentWebTrafficMonitorTaskStatus | Статус задачи Защита трафика: <b>Вкл.</b> – запущена; <b>Выкл.</b> – остановлена или приостановлена.                                                                               |

## Счетчик обновлений

Table 109. Счетчик обновлений

| Счетчик    | Определение                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------------------|
| avBasesAge | "Возраст" баз (промежуток времени в сотых долях секунды с момента создания последних установленных обновлений баз) |

## Счетчики постоянной защиты файлов

Table 110. *Счетчики постоянной защиты файлов*

| Счетчик                     | Определение                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| totalObjectsProcessed       | Общее количество проверенных объектов с момента последнего запуска задачи Постоянная защита файлов                                                                                                                                  |
| totalInfectedObjectsFound   | Общее количество обнаруженных зараженных и других объектов с момента последнего запуска задачи Постоянная защита файлов                                                                                                             |
| totalSuspiciousObjectsFound | Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска задачи Постоянная защита файлов                                                                                                             |
| totalVirusesFound           | Общее количество обнаруженных объектов с момента последнего запуска задачи Постоянная защита файлов                                                                                                                                 |
| totalObjectsQuarantined     | Общее количество зараженных, возможно зараженных и прочих объектов, которые программа Kaspersky Security для Windows Server поместила на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов      |
| totalObjectsNotQuarantined  | Общее количество зараженных или возможно зараженных объектов, которые программе Kaspersky Security для Windows Server не удалось поместить на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsDisinfected     | Общее количество зараженных объектов, которые вылечила программа Kaspersky Security для Windows Server; рассчитывается с момента последнего запуска задачи Постоянная защита файлов                                                 |
| totalObjectsNotDisinfected  | Общее количество зараженных и прочих объектов, которые программе Kaspersky Security для Windows Server не удалось вылечить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов                             |
| totalObjectsDeleted         | Общее количество зараженных, возможно зараженных и прочих объектов, которые удалила программа Kaspersky Security для Windows Server; рассчитывается с момента последнего запуска задачи Постоянная защита файлов                    |
| totalObjectsNotDeleted      | Общее количество зараженных, возможно зараженных и прочих объектов, которые программе Kaspersky Security для Windows Server не удалось удалить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов         |
| totalObjectsBackedUp        | Общее количество зараженных и прочих объектов, которые программа Kaspersky Security для Windows Server поместила в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов                 |
| totalObjectsNotBackedUp     | Общее количество зараженных и прочих объектов, которые программе Kaspersky Security для Windows Server не удалось поместить в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов      |

## Счетчики Проверки скриптов

Table 111. *Счетчики Проверки скриптов*

| Счетчик                            | Определение                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| totalScriptsProcessed              | Общее количество скриптов, проверенных с момента последнего запуска задачи Проверка скриптов                       |
| totalInfectedDangerousScriptsFound | Общее количество зараженных и опасных скриптов, обнаруженных с момента последнего запуска задачи Проверка скриптов |
| totalSuspiciousScriptsFound        | Общее количество возможно зараженных скриптов, обнаруженных с момента последнего запуска задачи Проверка скриптов  |
| totalScriptsBlocked                | Общее количество скриптов, заблокированных с момента последнего запуска задачи Проверка скриптов                   |

## Счетчики Защиты трафика

Table 112. *Счетчики Защиты трафика*

| Счетчик                                | Определение                                                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| wtTotalObjectsProcessed                | Общее количество объектов, обработанных с момента последнего запуска задачи Защита трафика                        |
| wtTotalInfectedObjectsFound            | Общее количество зараженных и прочих объектов, обнаруженных с момента последнего запуска задачи Защита трафика    |
| wtTotalVirusesFound                    | Общее количество объектов, обнаруженных с момента последнего запуска задачи Защита трафика                        |
| wtTotalPhishingResourcesAccess         | Общее количество попыток доступа к фишинговым ресурсам с момента последнего запуска задачи Защита трафика         |
| wtTotalURLProcessed                    | Общее количество веб-адресов, обработанных с момента последнего запуска задачи Защита трафика                     |
| wtTotalInfectedObjectsDownloadsBlocked | Общее количество загрузок зараженных объектов, заблокированных с момента последнего запуска задачи Защита трафика |

## SNMP-ловушки Kaspersky Security для Windows Server и их параметры

В Kaspersky Security для Windows Server предусмотрены следующие параметры SNMP-ловушек:

- eventThreatDetected: Обнаружен объект.  
В ловушке используются следующие параметры:
  - eventDateAndTime

- eventSeverity
- computerName
- userName
- objectName
- threatName
- detectType
- detectCertainty
- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в резервном хранилище превысил значение, заданное параметром **Максимальный размер резервного хранилища (МБ)**. Kaspersky Security для Windows Server продолжает резервировать зараженные объекты.

В ловушке используются следующие параметры:

- eventDateAndTime
- eventSeverity
- eventSource
- eventThresholdBackupStorageSizeExceeds: Достигнут порог свободного места в резервном хранилище. Объем свободного места в резервном хранилище меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Security для Windows Server продолжает резервировать зараженные объекты.

В ловушке используются следующие параметры:

- eventDateAndTime
- eventSeverity
- eventSource
- eventQuarantineStorageSizeExceeds: Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, заданное параметром **Максимальный размер карантина (МБ)**. Kaspersky Security для Windows Server продолжает помещать возможно зараженные объекты на карантин.

В ловушке используются следующие параметры:

- eventDateAndTime
- eventSeverity
- eventSource
- eventThresholdQuarantineStorageSizeExceeds: Достигнут порог свободного места в карантине. Объем свободного места в папке карантина меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Security для Windows Server продолжает резервировать зараженные объекты.

В ловушке используются следующие параметры:

- eventDateAndTime
- eventSeverity
- eventSource

- eventObjectNotQuarantined: Ошибка карантина.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- userName
- computerName
- objectName
- storageObjectNotAddedEventReason

- eventObjectNotBackured: Ошибка сохранения копии объекта в резервное хранилище.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- objectName
- userName
- computerName
- storageObjectNotAddedEventReason

- eventQuarantineInternalError: Внутренняя ошибка карантина.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- eventReason

- eventBackupInternalError: Ошибка резервного хранилища.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- eventReason

- eventAVBasesOutdated: Базы программы устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime

- eventSource
- days
- eventAVBasesTotallyOutdated: Базы программы сильно устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- days
- eventApplicationStarted: программа Kaspersky Security для Windows Server запущена.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- eventApplicationShutdown: программа Kaspersky Security для Windows Server остановлена.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей давно не выполнялась. Количество дней с момента последнего завершения задачи Проверка важных областей.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- days
- eventLicenseHasExpired: Срок действия лицензии истек.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- eventLicenseExpiresSoon: Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

В ловушке используются следующие параметры:

- eventSeverity

- eventDateAndTime
- eventSource
- days
- eventTaskInternalError: Ошибка выполнения задачи.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- errorCode
- knowledgeBaseId
- taskName
- eventUpdateError: Ошибка при выполнении задачи обновления.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- taskName
- updaterErrorEventReason

## Описания и возможные значения параметров SNMP-ловушек Kaspersky Security для Windows Server

Ниже приведено описание и допустимые значения параметров ловушек:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.

Параметр может принимать следующие значения:

- critical (1) – критический;
- warning (2) – предупреждение;
- info (3) – информационный.
- userName: имя пользователя (например, имя пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя защищаемого устройства (например, имя защищаемого устройства, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

Параметр может принимать следующие значения:

- unknown (0) – функциональный компонент не определен;
- quarantine (1) – Карантин;

- backup (2) – Резервное хранилище;
- reporting (3) – Журналы выполнения задач;
- updates (4) – Обновление;
- realTimeProtection (5) – Постоянная защита файлов;
- onDemandScanning (6) – Проверка по требованию;
- product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Security для Windows Server в целом;
- systemAudit (8) – Журнал системного аудита.

- eventReason: причина возникновения события.

Параметр может принимать следующие значения:

- reasonUnknown (0) – причина не определена.
- reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Security для Windows Server будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).
- threatName: имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название объекта, которое Kaspersky Security для Windows Server возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
- detectType: тип обнаруженного объекта.

Параметр может принимать следующие значения:

- undefined (0) – не определен;
- virware – классические вирусы и сетевые черви;
- trojware – троянские программы;
- malware – прочие вредоносные программы;
- adware – рекламные программы;
- pornware – порнографические программы;
- riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройству или личным данным.
- detectCertainty: степень уверенности обнаружения угрозы.

Параметр может принимать следующие значения:

- Suspicion (возможно зараженный) – программа Kaspersky Security для Windows Server обнаружила частичное совпадение участка кода объекта с известным участком вредоносного кода.
- Sure (зараженный) – программа Kaspersky Security для Windows Server обнаружила полное совпадение участка кода объекта с известным участком вредоносного кода.
- days: количество дней (например, количество дней до окончания срока действия лицензии).



- `errorCode`: код ошибки.
- `knowledgeBaseId`: адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
- `taskName`: название задачи.
- `updaterErrorEventReason`: причина ошибки обновления.

Параметр может принимать следующие значения:

- `reasonUnknown (0)` – причина не определена;
- `reasonAccessDenied` – доступ запрещен;
- `reasonUrlsExhausted` – список источников обновлений исчерпан;
- `reasonInvalidConfig` – неправильный файл конфигурации;
- `reasonInvalidSignature` – неверная подпись;
- `reasonCantCreateFolder` – невозможно создать папку;
- `reasonFileOperError` – файловая ошибка;
- `reasonDataCorrupted` – объект поврежден;
- `reasonConnectionReset` – сброс соединения;
- `reasonTimeOut` – истекло время ожидания при соединении;
- `reasonProxyAuthError` – ошибка проверки подлинности на прокси-сервере;
- `reasonServerAuthError` – ошибка проверки подлинности на сервере;
- `reasonHostNotFound` – устройство не найдено;
- `reasonServerBusy` – сервер недоступен;
- `reasonConnectionError` – ошибка соединения;
- `reasonModuleNotFound` – объект не найден;
- `reasonBlstCheckFailed(16)` – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.
- `storageObjectNotAddedEventReason`: причина, по которой объект не был помещен в резервное хранилище или на карантин.

Параметр может принимать следующие значения:

- `reasonUnknown (0)` – причина не определена.
- `reasonStorageInternalError` – ошибка базы данных; необходимо восстановление Kaspersky Security для Windows Server.
- `reasonStorageReadOnly` – база данных доступна только для чтения; необходимо восстановление Kaspersky Security для Windows Server.
- `reasonStorageIOError` – ошибка ввода-вывода: а) программа Kaspersky Security для Windows Server повреждена и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Security для Windows Server, поврежден.
- `reasonStorageCorrupted` – хранилище повреждено; необходимо восстановление Kaspersky Security для Windows Server.
- `reasonStorageFull` – база данных заполнена; требуется свободное место на диске.

- `reasonStorageOpenError` – не удается открыть файл базы данных; необходимо восстановление Kaspersky Security для Windows Server.
- `reasonStorageOSFeatureError` – некоторые особенности операционной системы не отвечают требованиям Kaspersky Security для Windows Server.
- `reasonObjectNotFound` – помещаемый на карантин объект отсутствует на диске.
- `reasonObjectAccessError` – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
- `reasonDiskOutOfSpace` – недостаточно места на диске.

## Интеграция с WMI

Kaspersky Security для Windows Server поддерживает интеграцию с инструментарием управления Windows (Windows Management Instrumentation, WMI): вы можете использовать клиентские системы, которые получают с помощью WMI данные по стандарту Web-Based Enterprise Management (WBEM), для получения данных о статусе программы Kaspersky Security для Windows Server и ее компонентов.

В момент установки Kaspersky Security для Windows Server регистрирует в системе собственный модуль для создания пространства имен Kaspersky Security для Windows Server на защищаемом устройстве. Пространство имен Kaspersky Security для Windows Server позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Security для Windows Server.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

*Непериодические задачи* – это задачи программы, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения. Результаты выполнения таких задач фиксируются непрерывно в ходе выполнения и представляют собой отдельные события (например, обнаружение зараженного объекта одной из задач постоянной защиты сервера). Задачами такого типа можно управлять с помощью политик Kaspersky Security Center.

*Периодические задачи* – это задачи программы, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде количества процентов. Результаты выполнения таких задач фиксируются по завершении задачи и представляют собой отдельный элемент или факт изменения состояния программы (например, завершение Обновления баз программы, сформированные конфигурационные файлы для задач автоматического формирования правил). На одном защищаемом устройстве одновременно может быть запущено несколько периодических задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять периодическими задачами с помощью групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из него динамические данные, вы сможете получить следующие данные о текущем состоянии программы.

Table 113. Данные о состоянии программы

| Свойство экземпляра класса | Описание                                                      | Значения                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProductName                | Название установленной программы.                             | Полное название программы без номера версии.                                                                                                                                                                                                                                                                                                                                          |
| ProductVersion             | Полный номер версии установленной программы.                  | Полный номер версии программы, включая номер сборки.                                                                                                                                                                                                                                                                                                                                  |
| InstalledPatches           | Набор отображаемых имен установленных патчей.                 | Перечень критических исправлений, установленных для программы.                                                                                                                                                                                                                                                                                                                        |
| IsLicenseInstalled         | Статус активации программы.                                   | Статус ключа, с помощью которого активирована программа.<br>Возможные значения: <ul style="list-style-type: none"> <li>False – В программе не добавлен лицензионный ключ.</li> <li>True - В программе добавлен лицензионный ключ.</li> </ul>                                                                                                                                          |
| LicenseDaysLeft            | Количество дней до истечения срока действия текущей лицензии. | Количество дней, оставшихся до истечения срока действия текущей лицензии.<br>Возможные неположительные значения: <ul style="list-style-type: none"> <li>0 - Срок действия лицензии истек.</li> <li>-1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по черному списку ключей).</li> </ul> |
| AVBasesDatetime            | Временная отметка для текущей версии антивирусных баз.        | Дата и время формирования антивирусных баз, используемых в текущий момент.<br>Если установленная программа не использует антивирусные базы, поле содержит значение "Not installed".                                                                                                                                                                                                   |
| IsExploitPreventionEnabled | Статус компонента Защита от эксплойтов.                       | Статус компонента Защита от эксплойтов.<br>Возможные значения: <ul style="list-style-type: none"> <li>True - Компонент Защита от эксплойтов включен и выполняет функции защиты.</li> <li>False - Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.</li> </ul>                                          |

| Свойство экземпляра класса | Описание                                                                                                                | Значения                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProtectionTasksRunning     | Набор запущенных задач защиты.                                                                                          | Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные непериодические задачи.<br>Если не запущена ни одна из непериодических задач, поле содержит значение "Нет".                                                                                                                                                                                         |
| IsAppControlRunning        | Статус выполнения задачи Контроль запуска программ.                                                                     | Статус выполнения задачи Контроль запуска программ.<br><ul style="list-style-type: none"> <li>• True - Задача Контроль запуска программ выполняется в текущий момент.</li> <li>• False - Задача Контроль запуска программ не выполняется в текущий момент или компонент Контроль запуска программ не установлен.</li> </ul>                                                                                                     |
| AppControlMode             | Режим работы задачи Контроль запуска программ.                                                                          | Описание текущего состояния компонента Контроль запуска программ, а также выбранного режима соответствующей задачи.<br>Возможные значения: <ul style="list-style-type: none"> <li>• Active - в параметрах задачи указан режим <b>Активный</b>.</li> <li>• Statistics Only - в параметрах задачи указан режим <b>Только статистика</b>.</li> <li>• Not installed - Компонент Контроль запуска программ не установлен.</li> </ul> |
| AppControlRulesNumber      | Общее количество правил контроля запуска программ.                                                                      | Количество правил, заданных в параметрах задачи Контроль запуска программ в текущий момент.                                                                                                                                                                                                                                                                                                                                     |
| AppControlLastBlocking     | Временная отметка последней блокировки запуска программы, выполненной задачей Контроль запуска программ в любом режиме. | Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима выполнения задачи.<br>Если на момент выполнения запроса WMI не зарегистрировано ни одного случая блокировки запуска программы, в поле отображается значение "Нет".                                                                        |

| Свойство экземпляра класса | Описание                                                                                   | Значения                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PeriodicTasksRunning       | Набор запущенных периодических задач.                                                      | Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны отображаться все запущенные периодические задачи.<br>Если не запущена ни одна из периодических задач, поле содержит значение "Нет".                                                                                                                            |
| ConnectionState            | Состояние соединения между компонентом Поставщик WMI и службой Kaspersky Security (KAVFS). | Информация о статусе соединения между компонентом Поставщик WMI и службой Kaspersky Security.<br>Возможные значения: <ul style="list-style-type: none"> <li>Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы.</li> <li>Failed. Error Code: &lt;code&gt; - Соединение не удалось установить из-за ошибки с указанным кодом.</li> </ul> |

Указанные данные являются свойствами экземпляра класса  
KasperskySecurity\_ProductInfo.ProductName=Kaspersky Security, где:

- KasperskySecurity\_ProductInfo – имя класса Kaspersky Security для Windows Server;
- .ProductName=Kaspersky Security – ключевой параметр Kaspersky Security для Windows Server.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

# Работа с Kaspersky Security для Windows Server из командной строки

Этот раздел содержит описание работы с Kaspersky Security для Windows Server из командной строки.

## В этом разделе

|                           |                     |
|---------------------------|---------------------|
| Команды.....              | <a href="#">694</a> |
| Коды возврата команд..... | <a href="#">725</a> |

## Команды

Вы можете выполнять основные команды управления Kaspersky Security для Windows Servers из командной строки при помощи компонента Утилита командной строки, который входит в набор программных компонентов Kaspersky Security для Windows Servers.

С помощью командной строки можно управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Security для Windows Server.

Некоторые из команд Kaspersky Security для Windows Server выполняются в следующих режимах:

- Синхронный режим: управление возвращается на Консоль только после завершения выполнения команды.
- Асинхронный режим: управление возвращается на Консоль сразу после запуска команды.

► *Чтобы прервать выполнение команды в синхронном режиме,*

нажмите комбинацию клавиш **CTRL+C**.

При вводе команд Kaspersky Security для Windows Server применяйте следующие правила:

- Вводите ключи и команды символами верхнего или нижнего регистра.
- Разделяйте ключи символом пробела.
- Если имя файла или папки содержит пробел, заключите путь к файлу или папке в кавычки, например: "C:\TEST\test cpp.exe".
- При необходимости можно использовать подстановочные символы в масках имен файлов или путей, например: "C:\Temp\Temp\*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp\*.doc".

С помощью командной строки можно выполнять все операции по управлению и администрированию Kaspersky Security для Windows Server (см. таблицу ниже).

Table 114. Команды Kaspersky Security для Windows Server

| Команда                                                                                                                                                | Описание                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL" на стр. <a href="#">709</a> )                | Обновляет список правил в соответствии с выбранным правилом импорта.                                                                            |
| KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачами Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG" на стр. <a href="#">706</a> )     | Задаёт режим работы задачи Контроль запуска программ.                                                                                           |
| KAVSHELL APPCONTROL /GENERATE (см. раздел "Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE" на стр. <a href="#">707</a> ) | Запускает задачу Формирование правил контроля запуска программ.                                                                                 |
| KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журналов Kaspersky Security для Windows Server. KAVSHELL VACUUM" на стр. <a href="#">718</a> )      | Дефрагментирует файлы журналов Kaspersky Security для Windows Server.                                                                           |
| KAVSHELL PASSWORD                                                                                                                                      | Управляет параметрами защиты паролем.                                                                                                           |
| KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Security для Windows Server. KAVSHELL HELP" на стр. <a href="#">697</a> )                | Отображает справку о командах Kaspersky Security для Windows Server.                                                                            |
| KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. <a href="#">697</a> )                 | Запускает службу Kaspersky Security.                                                                                                            |
| KAVSHELL STOP (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. <a href="#">697</a> )                  | Останавливает службу Kaspersky Security.                                                                                                        |
| KAVSHELL SCAN (см. раздел "Проверка выбранной области. KAVSHELL SCAN" на стр. <a href="#">698</a> )                                                    | Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами командной строки. |

| Команда                                                                                                                                     | Описание                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| KAVSHELL SCANCritical (см. раздел "Запуск задачи Проверка важных областей. KAVSHELL SCANCritical" на стр. <a href="#">702</a> )             | Запускает системную задачу Проверка важных областей.                                                                                                     |
| KAVSHELL TASK (см. раздел "Управление задачами в асинхронном режиме. KAVSHELL TASK" на стр. <a href="#">703</a> )                           | Запускает, приостанавливает, возобновляет, останавливает указанную задачу в асинхронном режиме. Возвращает текущее состояние задачи / статистику задачи. |
| KAVSHELL RTP (см. раздел "Запуск и остановка задач постоянной защиты сервера. KAVSHELL RTP" на стр. <a href="#">705</a> )                   | Запускает или останавливает все задачи постоянной защиты сервера.                                                                                        |
| KAVSHELL UPDATE (см. раздел "Запуск задачи Обновление баз программы. KAVSHELL UPDATE" на стр. <a href="#">710</a> )                         | Запускает задачу Обновление баз программы с параметрами, заданными ключами командной строки.                                                             |
| KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Security для Windows Server. KAVSHELL ROLLBACK" на стр. <a href="#">714</a> ) | Откатывает базы программы до предыдущей версии.                                                                                                          |
| KAVSHELL LICENSE (см. раздел "Активация программы. KAVSHELL LICENSE" на стр. <a href="#">714</a> )                                          | Добавляет или удаляет ключи и коды активации. Отображает информацию о добавленных ключах и кодах активации.                                              |
| KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE" на стр. <a href="#">715</a> )           | Включает или выключает запись журналов трассировки. Управляет параметрами журналов трассировки.                                                          |
| KAVSHELL DUMP (см. раздел "Включение и выключение создания файла дампа. KAVSHELL DUMP" на стр. <a href="#">719</a> )                        | Включает и выключает создание файлов дампов процессов Kaspersky Security для Windows Server при их аварийном завершении.                                 |
| KAVSHELL IMPORT (см. раздел "Импорт параметров. KAVSHELL IMPORT" на стр. <a href="#">720</a> )                                              | Импортирует общие параметры Kaspersky Security для Windows Server, а также параметры функций и задач из конфигурационного файла.                         |
| KAVSHELL EXPORT (см. раздел "Экспорт параметров. KAVSHELL EXPORT" на стр. <a href="#">721</a> )                                             | Экспортирует все параметры Kaspersky Security для Windows Server и существующих задач в конфигурационный файл.                                           |



| Команда                                                                                                                             | Описание                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| KAVSHELL DEVCONTROL<br>(см. раздел "Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL" на стр. <a href="#">710</a> ) | Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления. |

## Отображение справки о командах Kaspersky Security для Windows Server. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Security для Windows Server, выполните одну из следующих команд:

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

Чтобы получить описание команды и ее синтаксис, выполните одну из следующих команд:

```
KAVSHELL HELP <команда>
```

```
KAVSHELL <команда> /?
```

### Примеры команды KAVSHELL HELP

Чтобы просмотреть подробную информацию о команде KAVSHELL SCAN, выполните следующую команду:

```
KAVSHELL HELP SCAN
```

## Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP

Чтобы запустить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускается Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

## Проверка выбранной области. KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого устройства, используйте команду `KAVSHELL SCAN`. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная с помощью команды `KAVSHELL SCAN`, является временной. Она отображается в Консоли программы только во время выполнения (в Консоли программы не отображаются ее параметры). Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи.

При указании путей в задачах проверки отдельных областей можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду `KAVSHELL SCAN` с правами этого пользователя.

Команда `KAVSHELL SCAN` выполняется в синхронном режиме.

Чтобы запустить существующую задачу проверки по требованию из командной строки, используйте команду `KAVSHELL TASK` (см. раздел "Управление задачами в асинхронном режиме. KAVSHELL TASK" на стр. [703](#)).

### Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<имя файла со
списком областей проверки>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"маски">] [/ES:<размер>] [/ET:<количество секунд>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<дни>] [NORECALL]>]
[/NOICHECKER] [/NOISWIFT] [/ANALYZERLEVEL] [/W:<имя файла журнала выполнения
задачи>] [/ANSI] [/ALIAS:<альтернативное название задачи>]
```

У команды `KAVSHELL SCAN` есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

### Примеры команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\
C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED
/AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info"
/NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log

KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Table 115. Ключи / параметры команды KAVSHELL SCAN

| Ключ / параметр                                                                                                                                   | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Область проверки.</b> Обязательный параметр.                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <файлы>                                                                                                                                           | <p>Область проверки – список файлов, папок, сетевых путей и стандартных областей.</p> <p>Указывайте сетевые пути к формату UNC (Universal Naming Convention).</p> <p>В следующем примере папка Folder4 указана без пути к ней. Это значит, что она находится в папке, из которой вы запускаете команду KAVSHELL.</p> <p>KAVSHELL SCAN Folder4</p> <p>Если имя объекта, который вы хотите проверить, содержит пробелы, заключайте его в кавычки.</p> <p>Kaspersky Security для Windows Server проверит также все вложенные папки в выбранной папке.</p> <p>Для проверки группы файлов вы можете использовать символы * или ?.</p> |
| <папки>                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <сетевой путь>                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| /MEMORY                                                                                                                                           | Проверять объекты в оперативной памяти.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| /SHARED                                                                                                                                           | Проверять папки общего доступа на защищаемом устройстве.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| /STARTUP                                                                                                                                          | Проверять объекты автозапуска.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| /REMDRIVES                                                                                                                                        | Проверять съемные диски.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| /FIXDRIVES                                                                                                                                        | Проверять жесткие диски.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| /MYCOMP                                                                                                                                           | Проверять все области защищаемого устройства.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| /L: <путь к файлу со списком областей проверки>                                                                                                   | <p>Полный путь к файлу со списком областей проверки.</p> <p>Разделяйте области проверки в файле символом перевода строки. Вы можете указывать стандартные области проверки, как показано в следующем примере файла со списком областей проверки:</p> <p>C:\</p> <p>D:\Docs\*.doc</p> <p>E:\My Documents</p> <p>/STARTUP</p> <p>/SHARED</p>                                                                                                                                                                                                                                                                                       |
| <b>Проверяемые объекты</b> (типы файлов). Если вы не укажете этот ключ, Kaspersky Security для Windows Server будет проверять объекты по формату. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| /FA                                                                                                                                               | Проверять все объекты                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| /FC                                                                                                                                               | Проверять объекты по формату (по умолчанию). Kaspersky Security для Windows Server проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| /FE                                                                                                                                               | Проверять объекты по расширению. Kaspersky Security для Windows Server проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| /NEWONLY                                                                                                                                          | <p>Проверять только новые и измененные файлы.</p> <p>Если вы не укажете этот ключ, Kaspersky Security для Windows Server будет проверять все объекты.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Ключ / параметр                                                                                                                                                                                         | Описание                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Действия над зараженными и другими обнаруженными объектами.</b> Если вы не зададите никаких значений этого ключа, Kaspersky Security для Windows Server будет выполнять действие <b>Пропускать</b> . |                                                                                                                                                                                                                                                                                                                                                                         |
| DISINFECT                                                                                                                                                                                               | Лечить; если лечение невозможно, пропускать<br>Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Security для Windows Server для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Security для Windows Server не будет обрабатывать возможно зараженные объекты. |
| DISINFDEL                                                                                                                                                                                               | Лечить; если лечение невозможно, удалять                                                                                                                                                                                                                                                                                                                                |
| DELETE                                                                                                                                                                                                  | Удалять<br>Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Security для Windows Server для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Security для Windows Server не будет обрабатывать возможно зараженные объекты.                                     |
| REPORT                                                                                                                                                                                                  | Отсылать отчет (по умолчанию)                                                                                                                                                                                                                                                                                                                                           |
| AUTO                                                                                                                                                                                                    | Выполнять рекомендованное действие                                                                                                                                                                                                                                                                                                                                      |
| <b>/AS: Действия над возможно зараженными объектами.</b> Если вы не укажете этот параметр, Kaspersky Security для Windows Server будет выполнять действие <b>Пропускать</b> .                           |                                                                                                                                                                                                                                                                                                                                                                         |
| QUARANTINE                                                                                                                                                                                              | Карантин                                                                                                                                                                                                                                                                                                                                                                |
| DELETE                                                                                                                                                                                                  | Удалять                                                                                                                                                                                                                                                                                                                                                                 |
| REPORT                                                                                                                                                                                                  | Отсылать отчет (по умолчанию)                                                                                                                                                                                                                                                                                                                                           |
| AUTO                                                                                                                                                                                                    | Выполнять рекомендованное действие                                                                                                                                                                                                                                                                                                                                      |
| <b>Исключения</b>                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                         |
| /E:ABMSPO                                                                                                                                                                                               | Исключать составные объекты следующих типов:<br>А – SFX-архивы;<br>В – почтовые базы;<br>М – файлы почтовых форматов;<br>S – архивы (включая SFX-архивы);<br>Р – упакованные объекты;<br>О – вложенные OLE-объекты.                                                                                                                                                     |
| /EM:<"маски">                                                                                                                                                                                           | Исключать файлы по маске<br>Можно указать несколько масок, например: EM: "*.txt; *.png; C:\Videos\*.avi".                                                                                                                                                                                                                                                               |
| /ET:<количество секунд>                                                                                                                                                                                 | Прекращать обработку объекта, если она продолжается дольше указанного количества секунд.<br>По умолчанию ограничений продолжительности нет.                                                                                                                                                                                                                             |
| /ES:<размер>                                                                                                                                                                                            | Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанное значение.<br>По умолчанию Kaspersky Security для Windows Server проверяет объекты любого размера.                                                                                                                                                                              |

| Ключ / параметр                         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /TZOFF                                  | Отменить исключения доверенной зоны.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Дополнительные параметры (опции)</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| /NOICHECKER                             | Выключить использование технологии iChecker (по умолчанию включено).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| /NOISWIFT                               | Выключить использование технологии iSwift (по умолчанию включено).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| /ANALYZERLEVEL:<уровень анализа>        | <p>Включить использование эвристического анализатора, настроить уровень анализа.</p> <p>Доступны следующие уровни эвристического анализа:</p> <ul style="list-style-type: none"> <li>1 – поверхностный;</li> <li>2 – средний;</li> <li>3 – глубокий.</li> </ul> <p>Если вы опустите этот параметр, Kaspersky Security для Windows Server не будет использовать эвристический анализатор.</p>                                                                                                                                                                                                                                           |
| /ALIAS:<альтернативное название задачи> | <p>Присваивает задаче проверки по требованию временное название, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Security для Windows Server.</p> <p>Если этот параметр не задан, задаче присваивается временное название вида scan_&lt;kavshell_pid&gt;, например, scan_1234. В Консоли программы задаче присваивается название "Проверка объектов &lt;дата и время&gt;", например, "Проверка объектов 16.08.2007 17:13:14".</p> |
| Параметры журнала выполнения задачи     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Ключ / параметр                          | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /W:<имя файла журнала выполнения задачи> | <p>Если указан этот параметр, Kaspersky Security для Windows Server сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.</p> <p>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Security для Windows Server в оснастке "Просмотр событий".</p> <p>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли программы.</p> <p>Если Kaspersky Security для Windows Server не удастся создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.</p> |
| /ANSI                                    | <p>Этот параметр позволяет записывать события в журнал выполнения задачи в кодировке ANSI.</p> <p>Параметр ANSI не будет применяться, если не задан параметр W.</p> <p>Если параметр ANSI не указан, то журнал выполнения задачи формируется в кодировке UNICODE.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Запуск задачи Проверка важных областей. KAVSHELL SCANCritical

Используйте команду `KAVSHELL SCANCritical`, чтобы запустить задачу Проверка важных областей с параметрами, заданными в Консоли программы.

### Синтаксис команды KAVSHELL SCANCritical

`KAVSHELL SCANCritical [/W:<имя файла журнала выполнения задачи>]`

### Примеры команды KAVSHELL SCANCritical

Чтобы запустить задачу Проверка важных областей и сохранить журнал выполнения задачи в файле с именем `scancritical.log` в текущей папке, выполните следующую команду:

`KAVSHELL SCANCritical /W:scancritical.log`

С помощью параметра /W можно настроить местоположение файла журнала выполнения задачи (см. таблицу ниже).

Table 116. Синтаксис параметра /W команды KAVSHELL SCANCritical

| Ключ / параметр                          | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /W:<имя файла журнала выполнения задачи> | <p>Если указан этот параметр, Kaspersky Security для Windows Server сохранит файл журнала выполнения задачи с именем, заданным значением параметра.</p> <p>Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.</p> <p>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Security для Windows Server в оснастке "Просмотр событий".</p> <p>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле <b>Журналы выполнения задач</b> в Консоли программы.</p> <p>Если Kaspersky Security для Windows Server не удастся создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.</p> |

## Управление задачами в асинхронном режиме. KAVSHELL TASK

Команда KAVSHELL TASK позволяет управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное название задачи> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS>]
```

### Примеры команды KAVSHELL TASK

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

```
KAVSHELL TASK network-attack-blocker /START
```

Команда `KAVSHELL TASK` может быть выполнена как без ключей/параметров, так и с использованием одного либо нескольких ключей/параметров (см. таблицу ниже).

Table 117. Ключи / параметры команды `KAVSHELL TASK`

| Ключ / параметр                  | Описание                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Без параметров                   | Возвращает список всех существующих задач Kaspersky Security для Windows Server. Список содержит следующие поля: альтернативное название задачи, категория задачи (системная или пользовательская) и текущий статус задачи.                                                                                                                                |
| <альтернативное название задачи> | Вместо названия задачи в команде <code>SCAN TASK</code> используйте ее альтернативное название – дополнительное сокращенное название, которое Kaspersky Security для Windows Server присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Security для Windows Server, введите команду <code>KAVSHELL TASK</code> без параметров. |
| <code>/START</code>              | Запустить указанную задачу в асинхронном режиме                                                                                                                                                                                                                                                                                                            |
| <code>/STOP</code>               | Остановить указанную задачу                                                                                                                                                                                                                                                                                                                                |
| <code>/PAUSE</code>              | Приостановить указанную задачу                                                                                                                                                                                                                                                                                                                             |
| <code>/RESUME</code>             | Возобновить указанную задачу в асинхронном режиме                                                                                                                                                                                                                                                                                                          |
| <code>/STATE</code>              | Получить текущее состояние задачи (например, <i>Выполняется</i> , <i>Завершена</i> , <i>Приостановлена</i> , <i>Остановлена</i> , <i>Завершена с ошибкой</i> , <i>Запускается</i> , <i>Восстанавливается</i> ).                                                                                                                                            |
| <code>/STATISTICS</code>         | Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи                                                                                                                                                                                                                                                     |

Обратите внимание, что не все задачи Kaspersky Security для Windows Server поддерживают ключи `/PAUSE`, `/RESUME` и `/STATE`.

Коды возврата команды `KAVSHELL TASK` (на стр. [727](#)).



## Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG

Команда `KAVSHELL CONFIG` позволяет удалить атрибут защищенного процесса (Protected Process Light) у службы Kaspersky Security с помощью драйвера ELAM, установленного во время установки программы.

### Синтаксис команды KAVSHELL CONFIG

`KAVSHELL CONFIG /PPL:<OFF>`

Table 118. Ключи / параметры команды KAVSHELL CONFIG

| Ключ / параметр       | Описание                                        |
|-----------------------|-------------------------------------------------|
| <code>/PPL:OFF</code> | Снять атрибут PPL со службы Kaspersky Security. |

## Запуск и остановка задач постоянной защиты сервера. KAVSHELL RTP

Команда `KAVSHELL RTP` позволяет запустить или остановить все задачи постоянной защиты сервера.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[ /pwd:<пароль> ]`.

### Синтаксис команды KAVSHELL RTP

`KAVSHELL RTP </START | /STOP>`

### Примеры команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты сервера, выполните следующую команду:

`KAVSHELL RTP /START`

Команда `KAVSHELL RTP` должна включать один из двух параметров (см. таблицу ниже).

Table 119. Параметры команды KAVSHELL RTP

| Ключ / параметр     | Описание                                                                                                         |
|---------------------|------------------------------------------------------------------------------------------------------------------|
| <code>/START</code> | Запустить все задачи постоянной защиты сервера: Постоянная защита файлов, Проверка скриптов и Использование KSN. |
| <code>/STOP</code>  | Остановить все задачи постоянной защиты сервера.                                                                 |

## Управление задачами Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG

Команда KAVSHELL APPCONTROL /CONFIG позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

### Синтаксис команды KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config  
/savetofile:<полный путь к XML файлу>
```

### Примеры команды KAVSHELL APPCONTROL /CONFIG

- Чтобы запустить задачу Контроль запуска программ в режиме **Активный** без контроля загрузки DLL-модулей и сохранить параметры задачи по завершении, выполните следующую команду:

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>  
/savetofile:c:\appcontrol\config.xml
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Table 120. Ключи / параметры команды KAVSHELL APPCONTROL /CONFIG

| Ключ / параметр                          | Описание                                                                                                                                                                                                                                                                 |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /mode:<applyrules statistics>            | Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: <ul style="list-style-type: none"> <li>active - применяются правила контроля запуска программ;</li> <li>statistics - только формировать статистику.</li> </ul> |
| /dll:<no yes>                            | Выключить или включить контроль загрузки DLL-модулей.                                                                                                                                                                                                                    |
| /savetofile: <путь к xml-файлу>          | Экспортировать заданные правила в указанный файл в формате XML.                                                                                                                                                                                                          |
| /savetofile: <полное имя xml-файла>      | Сохранить список правил в файл.                                                                                                                                                                                                                                          |
| /savetofile: <полное имя xml-файла> /sdc | Сохранить список правил контроля распространения программного обеспечения в файл.                                                                                                                                                                                        |
| /clearsdc                                | Удалить все правила контроля распространения программного обеспечения.                                                                                                                                                                                                   |

## Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE

Команда KAVSHELL APPCONTROL /GENERATE позволяет формировать списки правил контроля запуска программ.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <путь к папке> | /source:<путь к файлу со  
списком папок> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong]  
[/user:<пользователь или группа пользователей>] [/export:<полный путь к XML  
файлу>] [/import:<a|r|m>] [/prefix:<префикс для названий правил>] [/unique]
```

### Примеры команды KAVSHELL APPCONTROL /GENERATE

- Чтобы сформировать правила для файлов из указанных папок, выполните команду:

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt  
/export:c:\rules\appctrlrules.xml
```

- Чтобы сформировать правила для исполняемых файлов с любыми расширениями, хранящихся в указанной папке, и по завершении задачи сохранить сформированные правила в указанный XML-файл, выполните следующую команду:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms  
/export:c:\rules\appctrlrules.xml
```

Вы можете использовать ключи/параметры для настройки автоматического формирования правил задачи Контроль запуска программ (см. таблицу ниже).

Table 121. Ключи / параметры команды KAVSHELL APPCONTROL /GENERATE

| Ключ / параметр                                                                               | Описание                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Область применения разрешающих правил</b>                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <путь к папке>                                                                                | Указать путь к папке с исполняемыми файлами, для которых будут автоматически формироваться разрешающие правила.                                                                                                                                                                                                                                                                                                   |
| /source: <путь к файлу со списком папок>                                                      | Указать путь к TXT-файлу со списком папок, содержащих исполняемые файлы, для которых будут автоматически формироваться разрешающие правила.                                                                                                                                                                                                                                                                       |
| /masks: <edms>                                                                                | <p>Указать расширения исполняемых файлов, для которых будут автоматически формироваться разрешающие правила.</p> <p>В область применения правил можно включить файлы со следующими расширениями:</p> <ul style="list-style-type: none"> <li>• e - файлы с расширением exe;</li> <li>• d - файлы с расширением dll;</li> <li>• m - файлы с расширением msi;</li> <li>• s - скрипты.</li> </ul>                     |
| /runapp                                                                                       | Учитывать при формировании разрешающих правил программы, запущенные на защищаемом устройстве в текущий момент.                                                                                                                                                                                                                                                                                                    |
| <b>Действия при автоматическом формировании разрешающих правил</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                   |
| /rules: <ch cp h>                                                                             | <p>Указать действия при формировании разрешающих правил для задачи Контроль запуска программ:</p> <ul style="list-style-type: none"> <li>• ch – использовать цифровой сертификат. Если сертификат отсутствует, использовать SHA256-хеш.</li> <li>• cp — использовать цифровой сертификат. Если сертификат отсутствует, использовать путь к исполняемому файлу.</li> <li>• h – использовать SHA256-хеш.</li> </ul> |
| /strong                                                                                       | Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании разрешающих правил для задачи Контроль запуска программ. Команда выполняется, если указан параметр /rules: <ch cp>.                                                                                                                                                                                                      |
| /user: <пользователь или группа пользователей>                                                | Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или группой.                                                                                                                                                                                                                               |
| <b>Действия по завершении выполнения задачи Формирование правил контроля запуска программ</b> |                                                                                                                                                                                                                                                                                                                                                                                                                   |
| /export: <путь к XML-файлу>                                                                   | Сохранить сформированные правила в XML-файл.                                                                                                                                                                                                                                                                                                                                                                      |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /unique                                | Добавлять информацию о защищаемом устройстве, по программам которого формируются разрешающие правила контроля запуска программ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| /prefix: <префикс для названий правил> | Указать префикс названий разрешающих правил контроля запуска программ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| /import: <a r m>                       | <p>Импортировать сформированные правила в указанный список правил контроля запуска программ в соответствии с выбранным принципом добавления новых правил:</p> <ul style="list-style-type: none"> <li>• <b>a – Добавлять к существующим правилам</b> (одинаковые правила дублируются);</li> <li>• <b>r – Заменять существующие правила</b> (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален);</li> <li>• <b>m – Объединять с существующими правилами</b> (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).</li> </ul> |

## Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL

Команда KAVSHELL APPCONTROL позволяет добавлять правила из XML-файла в список правил задачи Контроль запуска программ в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

### Пример команды KAVSHELL APPCONTROL

- Чтобы добавить к имеющимся правилам контроля запуска программ правила из XML-файла по принципу *Добавить к существующим правилам*, выполните команду:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля запуска программ (см. таблицу ниже).

Table 122. Ключи / параметры команды KAVSHELL APPCONTROL

| Ключ / параметр                    | Описание                                                                                                                                                                                                                                                          |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /append <полный путь к XML файлу>  | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – <b>Добавить к существующим правилам</b> (одинаковые правила дублируются).                                                                                  |
| /replace <полный путь к XML файлу> | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – <b>Заменять существующие правила</b> (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален). |
| /merge <полный путь к XML файлу>   | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – <b>Объединить правила с существующими</b> (новые правила не дублируют существующие правила).                                                               |
| /clear                             | Очистить список правил контроля запуска программ.                                                                                                                                                                                                                 |

## Запуск задачи Обновление баз программы. KAVSHELL UPDATE

Команда KAVSHELL UPDATE позволяет запускать задачу обновления баз Kaspersky Security для Windows Server в синхронном режиме.

Задача Обновление баз программы, запущенная с помощью команды KAVSHELL UPDATE, является временной. Она отображается в Консоли программы только во время ее выполнения. Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, и к задачам обновления, созданным в Консоли программы, могут применяться политики Kaspersky Security Center. Сведения об использовании Kaspersky Security Center для управления Kaspersky Security для Windows Server на защищаемых устройствах приведены в разделе "Управление Kaspersky Security для Windows Server с помощью Kaspersky Security Center".

Чтобы указать путь к источнику обновлений в этой задаче, можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду KAVSHELL UPDATE с правами этого пользователя.

### Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE <Путь к источнику обновления | /AK | /KL> [/NOUSEKL]
[/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>]
[/PROXYPWD:<пароль>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<количество секунд>] [/REG:<код iso3166>] [/W:<имя
файла журнала выполнения задачи>] [/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL UPDATE есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

## Пример команды KAVSHELL UPDATE

- Чтобы запустить пользовательскую задачу Обновление баз программы, выполните следующую команду:

```
KAVSHELL UPDATE
```

- Чтобы запустить задачу Обновление баз программы, файлы обновлений для которой хранятся в сетевой папке \\server\databases, выполните следующую команду:

```
KAVSHELL UPDATE \\server\bases
```

- Чтобы запустить задачу Обновление баз программы с FTP-сервера <ftp://dnl-ru1.kaspersky-labs.com/> и записать все события задачи в файл c:\update\_report.log, выполните следующую команду:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- Чтобы загрузить обновления баз Kaspersky Security для Windows Server с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений с помощью прокси-сервера (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к защищаемому устройству с помощью встроенной в Windows проверки подлинности NTLM с именем пользователя netuser и паролем 123456, выполните следующую команду:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1  
/PROXYUSER:inetuser /PROXYPWD:123456
```

При использовании данного способа обновлений программа выходит из сертифицированного состояния.

Table 123. Ключи / параметры команды KAVSHELL UPDATE

| Ключ / параметр                                                                                                                                                                                                                  | Описание                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Источник обновления</b> (обязательный параметр). Укажите один или несколько источников. Kaspersky Security для Windows Server будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела. |                                                                                                                    |
| <путь в формате UNC>                                                                                                                                                                                                             | Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC.                          |
| <URL>                                                                                                                                                                                                                            | Пользовательские источники обновления. Адрес HTTP- или FTP-сервера, на котором располагается папка с обновлениями. |
| <Локальная папка>                                                                                                                                                                                                                | Пользовательские источники обновления. Папка на защищаемом устройстве.                                             |
| /AK                                                                                                                                                                                                                              | Использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений.                   |
| /KL                                                                                                                                                                                                                              | Использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.                         |

| Ключ / параметр                 | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /NOUSEKL                        | Не использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны (по умолчанию).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Параметры прокси-сервера</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| /PROXY:<адрес>:<порт>           | Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот параметр, Kaspersky Security для Windows Server будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| /AUTHTYPE:<0-2>                 | <p>Этот параметр задает метод аутентификации для доступа к прокси-серверу. Он может принимать следующие значения:</p> <p><b>0</b> – проверка подлинности NTLM в Microsoft Windows; Kaspersky Security для Windows Server обращается к прокси-серверу с использованием учетной записи <b>Локальная система (SYSTEM)</b>.</p> <p><b>1</b> – проверка подлинности NTLM в Microsoft Windows; Kaspersky Security для Windows Server обращается к прокси-серверу с использованием учетной записи, имя пользователя и пароль которой заданы параметрами /PROXYUSER и /PROXYPWD.</p> <p><b>2</b> – обычная проверка подлинности по имени пользователя и паролю, заданным параметрами /PROXYUSER и /PROXYPWD.</p> <p>Если для доступа к прокси-серверу не требуется аутентификация, можно не указывать этот параметр.</p> |
| /PROXYUSER:<имя пользователя>   | Имя пользователя, используемое для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| /PROXYPWD:<пароль>              | Пароль пользователя, используемый для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если указан параметр /PROXYUSER, но не указан параметр /PROXYPWD, считается, что задан пустой пароль.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| /NOPROXYFORKL                   | Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| /USEPROXYFORCUSTOM              | Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используется).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| /USEPROXYFORLOCAL               | Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение <b>Не использовать прокси-сервер для локальных адресов</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



| Ключ / параметр                            | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Общие параметры FTP- и HTTP-сервера</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| /NOFTPPASSIVE                              | Если указан этот ключ, Kaspersky Security для Windows Server использует активный режим FTP-сервера для соединения с защищаемым устройством. Если вы не укажете этот ключ, Kaspersky Security для Windows Server использует пассивный режим FTP-сервера, при возможности.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| /TIMEOUT:<количество секунд>               | Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот параметр, Kaspersky Security для Windows Server использует значение по умолчанию: 10 секунд. Значение параметра должно быть целым числом.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| /REG:<код iso3166>                         | Региональные параметры. Этот параметр используется при получении обновлений с серверов обновлений Лаборатории Касперского. Kaspersky Security для Windows Server минимизирует нагрузку на защищаемое устройство, выбирая ближайший к нему сервер обновлений.<br><br>Значение этого параметра должно быть двухбуквенным кодом страны, в которой расположено защищаемое устройство, в стандарте ISO 3166-1, например: /REG: gr или /REG:US. Если ключ не указан или указан недопустимый код страны, Kaspersky Security для Windows Server распознает местоположение защищаемого устройства в соответствии с региональными параметрами защищаемого устройства, на котором установлена Консоль программы.                                                                                                                                                                                                                                                                                                                                                                                                        |
| /ALIAS:<альтернативное название задачи>    | Этот параметр позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Security для Windows Server.<br><br>Если этот ключ не задан, задаче присваивается временное название вида update_<kavshell_pid>, например, update_1234. В Консоли программы задаче присваивается название "Обновление баз программы <дата и время>", например: "Обновление баз программы 16.08.2007 17:41:02".                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| /W:<имя файла журнала выполнения задачи>   | Если указан этот параметр, Kaspersky Security для Windows Server сохранит файл журнала выполнения задачи с именем, заданным значением параметра.<br><br>Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.<br><br>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Security для Windows Server в оснастке "Просмотр событий".<br><br>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.<br><br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br><br>Вы можете просматривать файл журнала во время выполнения задачи.<br><br>Журнал отображается в узле <b>Журналы выполнения задач</b> в Консоли программы.<br><br>Если Kaspersky Security для Windows Server не удастся создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке. |

Коды возврата команды KAVSHELL UPDATE (на стр. [728](#)).

## Откат обновления баз Kaspersky Security для Windows Server. KAVSHELL ROLLBACK

Команда `KAVSHELL ROLLBACK` позволяет выполнить системную задачу Откат обновления баз программы – откатить базы Kaspersky Security для Windows Server до предыдущей установленной версии. Команда выполняется синхронно.

### Синтаксис команды

`KAVSHELL ROLLBACK`

Коды возврата команды `KAVSHELL ROLLBACK` (на стр. [728](#)).

## Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR

Команда `KAVSHELL TASK LOG-INSPECTOR` позволяет осуществлять контроль целостности среды, основываясь на анализе журнала событий Windows.

### Синтаксис команды

`KAVSHELL TASK LOG-INSPECTOR`

### Пример команды

`KAVSHELL TASK LOG-INSPECTOR /stop`

Table 124. Ключи / параметры команды `KAVSHELL TASK LOG-INSPECTOR`

| Ключ / параметр          | Описание                                                                                                                                                                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/START</code>      | Запустить указанную задачу в асинхронном режиме                                                                                                                                                                 |
| <code>/STOP</code>       | Остановить указанную задачу                                                                                                                                                                                     |
| <code>/STATE</code>      | Получить текущее состояние задачи (например, <i>Выполняется</i> , <i>Завершена</i> , <i>Приостановлена</i> , <i>Остановлена</i> , <i>Завершена с ошибкой</i> , <i>Запускается</i> , <i>Восстанавливается</i> ). |
| <code>/STATISTICS</code> | Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи.                                                                                                         |

Коды возврата команды `KAVSHELL TASK LOG-INSPECTOR` (на стр. [726](#)).

## Активация программы. KAVSHELL LICENSE

Команда `KAVSHELL LICENSE` позволяет управлять ключами и кодами активации Kaspersky Security для Windows Server.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[ /pwd:<пароль> ]`.

Синтаксис команды KAVSHELL LICENSE

KAVSHELL LICENSE [/ADD:<файл ключа | код активации> [/R] | /DEL:<ключ | код активации>]

Примеры команды KAVSHELL LICENSE

► Чтобы активировать программу, выполните команду:

KAVSHELL.EXE LICENSE / ADD: <код активации или файл ключа>

► Чтобы получить информацию о добавленных ключах, выполните команду:

KAVSHELL LICENSE

► Чтобы удалить добавленный ключ с номером 0000-000000-00000001, выполните команду:

KAVSHELL LICENSE /DEL:0000-000000-00000001

Команда KAVSHELL LICENSE может быть выполнена как без ключей, так и с их использованием (см. таблицу ниже).

Table 125. Ключи / параметры команды KAVSHELL LICENSE

| Параметр                                 | Описание                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Без ключей                               | Команда возвращает следующую информацию о добавленных ключах: <ul style="list-style-type: none"><li>• Ключ.</li><li>• Тип лицензии (коммерческая).</li><li>• Срок действия связанной с ключом лицензии.</li><li>• Статус ключа (активный или дополнительный). Если значение статуса *, ключ добавлен в качестве дополнительного.</li></ul> |
| /ADD:<имя файла ключа или код активации> | Добавить ключ с помощью указанного файла или кода активации. Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.                                                                                                                          |
| /R                                       | Код активации или ключ /R является дополнительным к коду активации или ключу /ADD и указывает, что код активации или ключ добавляется в качестве дополнительного.                                                                                                                                                                          |
| /DEL:<ключ или код активации>            | Удалить указанный ключ или код активации.                                                                                                                                                                                                                                                                                                  |

Коды возврата команды KAVSHELL LICENSE (на стр. [729](#)).

Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE

Команда KAVSHELL TRACE позволяет включать или выключать ведение журнала трассировки всех подсистем Kaspersky Security для Windows Server, а также устанавливать уровень детализации информации в журнале.

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

## Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<папка с файлами журнала трассировки>  
[/S:<максимальный размер файла журнала в мегабайтах>  
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Если ведется журнал трассировки и вы хотите изменить его параметры, введите команду KAVSHELL TRACE с ключом /ON и с помощью ключей /S и /LVL задайте параметры журнала трассировки (см. таблицу ниже).

Table 126. Ключи / параметры команды KAVSHELL TRACE

| Ключ                                                 | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /ON                                                  | Включить ведение журнала трассировки.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| /F:<папка с файлами журнала трассировки>             | <p>Этот параметр указывает полный путь к папке, в которую будут сохранены файлы журнала трассировки (обязательный).</p> <p>Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Пути к папкам на сетевых дисках других защищаемых устройств указывать нельзя.</p> <p>Если указанный параметром путь содержит пробел, заключите его в кавычки, например: /F:"C:\Trace Folder".</p> <p>Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p> |
| /S: <максимальный размер файла журнала в мегабайтах> | <p>Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Security для Windows Server начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.</p> <p>Если значение этого параметра не указано, максимальный размер одного файла журнала составит 50 МБ.</p>                                                                                                                                                                                                                      |
| /LVL:debug info warning error critical               | <p>Этот параметр устанавливает уровень детализации журнала от максимального (<b>Вся отладочная информация</b>), при котором в журнал записываются все события, до минимального (<b>Критические события</b>), при котором в журнал записываются только критические события.</p> <p>Если значение этого параметра не указано, в журнал трассировки будут записываться все события с уровнем детализации <b>Вся отладочная информация</b>.</p>                                                                                                                                                       |
| /OFF                                                 | Этот параметр выключает ведение журнала трассировки.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Примеры команды KAVSHELL TRACE

- Чтобы включить ведение журнала трассировки с уровнем детализации **Вся отладочная информация** и максимальным размером файла журнала 200 МБ и сохранить файл журнала в папке C:\Trace Folder, выполните команду:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

- Чтобы включить ведение журнала трассировки с уровнем детализации **Важные события** и сохранить файл журнала в папку C:\Trace Folder, выполните команду:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

- Чтобы выключить ведение журнала трассировки, выполните команду:

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE (на стр. [729](#)).

## Дефрагментация файлов журнала Kaspersky Security для Windows Server. KAVSHELL VACUUM

Команда `KAVSHELL VACUUM` позволяет выполнить дефрагментацию файлов журнала программы. Это помогает избежать системных ошибок и ошибок программы из-за хранения большого количества файлов журнала, сформированных на основе событий программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Рекомендуется применять команду `KAVSHELL VACUUM` для оптимизации хранения файлов журналов в случае частых запусков задач проверки по требованию и задач обновления. При выполнении команды Kaspersky Security для Windows Server обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом устройстве по указанному пути.

По умолчанию файлы журнала программы сохраняются в папку `C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\11\Reports`. Если вы вручную указали другой путь для хранения файлов журнала, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журнала Kaspersky Security для Windows Server.

Файлы большого размера увеличивают время, необходимое команде `KAVSHELL VACUUM` на выполнение дефрагментации.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля сервера. Процедура дефрагментации блокирует доступ к журналу Kaspersky Security для Windows Server и запрещает запись событий в журнал. Чтобы избежать снижения защиты, рекомендуется планировать запуск команды `KAVSHELL VACUUM`.

- Чтобы выполнить дефрагментацию файлов журнала Kaspersky Security для Windows Server, выполните команду:

```
KAVSHELL VACUUM
```

Для выполнения команды необходимы права учетной записи Локальная система (Local System).

## Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Security для Windows Server использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Security для Windows Server создает файлы klamfb.dat и klamfb2.dat в папке %SYSTEMDRIVE%\System Volume Information. Эти файлы содержат информацию о проверенных незагрязненных объектах. Размер файла klamfb.dat (klamfb2.dat) увеличивается пропорционально количеству файлов, проверенных Kaspersky Security для Windows Server. В этом файле хранится только актуальная информация о существующих в системе файлах: если файл был удален, то Kaspersky Security для Windows Server удаляет информацию о нем из файла klamfb.dat.

Для очистки данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла klamfb.dat с помощью команды `KAVSHELL FBRESET`, Kaspersky Security для Windows Server не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Security для Windows Server может увеличить нагрузку на защищаемое устройство. При этом после очистки файла klamfb.dat Kaspersky Security для Windows Server проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Security для Windows Server заново добавляет информацию о каждом проверенном объекте в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не проверять файл повторно, если он не был изменен.

Для выполнения команды `KAVSHELL FBRESET` нужно запускать интерпретатор командной строки с правами учетной записи `SYSTEM`.

## Включение и выключение создания файла дампа. KAVSHELL DUMP

Команда `KAVSHELL DUMP` позволяет включать и выключать создание образов памяти (файлов дампов) процессов Kaspersky Security для Windows Server при их аварийном завершении (см. таблицу ниже). Кроме того, можно в любой момент создать дамп памяти для выполняющихся процессов Kaspersky Security для Windows Server.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена с правами учетной записи локальной системы (`SYSTEM`).

Kaspersky Security для Windows Server записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

Синтаксис команды KAVSHELL DUMP

KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом дампа> / P:<pid> | /OFF>

Table 127. Ключи / параметры команды KAVSHELL DUMP

| Ключ                        | Описание                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /ON                         | Включить создание файлов дампов памяти при аварийном завершении процесса.                                                                                                                                                                                                                                                                |
| /F:<папка с файлами дампов> | Это обязательный параметр. Указывает путь к папке, в которой будет сохранен файл дампа. Нельзя указывать пути к папкам на сетевых дисках других незащищенных устройств.<br>При указании пути к папке с файлом дампа памяти можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя. |
| /SNAPSHOT                   | Снимает образ памяти выполняющегося процесса с указанным идентификатором и сохраняет файл дампа в папку, указанную параметром /F.                                                                                                                                                                                                        |
| /P                          | Идентификатор процесса (PID); отображается в Диспетчере задач Microsoft Windows.                                                                                                                                                                                                                                                         |
| /OFF                        | Выключить создание файлов дампов памяти при аварийном завершении процесса.                                                                                                                                                                                                                                                               |

Коды возврата команды KAVSHELL DUMP (на стр. [730](#)).

Примеры команды KAVSHELL DUMP

- Чтобы включить создание файла дампа и сохранить файл дампа в папку C:\Dump Folder, выполните команду:

KAVSHELL DUMP /ON /F:"C:\Dump Folder"

- Чтобы снять образ памяти процесса с идентификатором 1234 в папку C:\Dumps, выполните команду:

KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234

- Чтобы выключить создание файлов дампа, выполните команду:

KAVSHELL DUMP /OFF

Импорт параметров. KAVSHELL IMPORT

Команда KAVSHELL IMPORT позволяет импортировать параметры Kaspersky Security для Windows Server и текущих задач из конфигурационного файла в Kaspersky Security для Windows Server на защищаемом устройстве. Вы можете создать конфигурационный файл с помощью команды KAVSHELL EXPORT.



Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL IMPORT

KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>

### Пример команды KAVSHELL IMPORT

KAVSHELL IMPORT Host1.xml

Table 128. Параметр команды KAVSHELL IMPORT

| Параметр                                     | Описание                                                                                                                                                                                                               |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |

Коды возврата команды KAVSHELL IMPORT (на стр. [731](#)).

## Экспорт параметров. KAVSHELL EXPORT

Команда KAVSHELL EXPORT позволяет экспортировать все параметры Kaspersky Security для Windows Server и его существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Security для Windows Server на других защищаемых устройствах.

### Синтаксис команды KAVSHELL EXPORT

KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>

### Пример команды KAVSHELL EXPORT

KAVSHELL EXPORT Host1.xml

Table 129. Параметр команды KAVSHELL EXPORT

| Параметр                                     | Описание                                                                                                                                                                                                                                                                   |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, в котором будут сохранены параметры. Конфигурационному файлу можно присвоить любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |

Коды возврата команды KAVSHELL EXPORT (на стр. [731](#)).

## Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

Команда KAVSHELL OMSINFO позволяет просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами и службой KSN. Информация об угрозах поступает из доступных журналов событий.

### Синтаксис команды KAVSHELL OMSINFO

KAVSHELL OMSINFO <полный путь к сформированному файлу с именем файла>

### Пример команды KAVSHELL OMSINFO

KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json

Table 130. Параметр команды KAVSHELL OMSINFO

| Параметр                                      | Описание                                                                                                  |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <путь к сформированному файлу с именем файла> | Имя сформированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах. |

## Управление задачами Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE

Команда KAVSHELL FIM /BASELINE позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL FIM /BASELINE

KAVSHELL FIM /BASELINE [/CREATE: [<область мониторинга> | /L:<путь к TXT-файлу со списком областей мониторинга>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/EXPORT:<путь к TXT-файлу> [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SHOW [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SCAN [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/PWD:<пароль>]

### Примеры команды KAVSHELL FIM /BASELINE

► Чтобы удалить эталон, выполните следующую команду:

KAVSHELL FIM /BASELINE /CLEAR /BL:<идентификатор эталона>

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Table 131. Ключи / параметры команды KAVSHELL FIM/ BASELINE

| Ключ / параметр | Описание                                                                                                                                                                                                                                                   |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /CREATE         | Создать задачу Мониторинг целостности файлов на основе эталона.<br><br>Kaspersky Security для Windows Server запустит новую задачу Мониторинг целостности файлов на основе эталона, чтобы создать эталон.                                                  |
| /L              | Укажите путь к TXT-файлу, содержащему список областей мониторинга.                                                                                                                                                                                         |
| /MD5            | Укажите алгоритм MD5 для расчета контрольной суммы (необязательный параметр).<br>Параметр /MD5 не используется совместно с параметром /SHA256.<br>Алгоритм MD5 используется по умолчанию.                                                                  |
| /SHA256         | Укажите алгоритм SHA256 для расчета контрольной суммы (необязательный параметр).<br>Параметр /SHA256 не используется совместно с параметром /MD5.<br>Алгоритм MD5 используется по умолчанию.                                                               |
| /SF             | Включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона (необязательный параметр).<br>По умолчанию вложенные папки не входят в область задачи Мониторинг целостности файлов на основе эталона.                       |
| /CLEAR          | Удалить эталон с указанным <идентификатором эталона> или эталон задачи с указанным <существующим названием>.<br>Удалить все эталоны, если не указан ни один из параметров <идентификатор эталона> или <существующее название>.<br>Необязательный параметр. |
| /BL             | Укажите уникальный идентификатор эталона (необязательный параметр).                                                                                                                                                                                        |
| /EXPORT         | Экспортировать данные всех эталонов в TXT-файл.                                                                                                                                                                                                            |
| /SHOW           | Показать данные всех эталонов.                                                                                                                                                                                                                             |
| /SCAN           | Запустить новую задачу Мониторинг целостности файлов на основе эталона с указанным <идентификатором эталона> или <существующим названием>.                                                                                                                 |

|                                                    |                                                                                                                                                                                                    |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /ALIAS                                             | Укажите название новой или существующей задачи.                                                                                                                                                    |
| <область мониторинга>                              | <p>Укажите файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.</p> <p>Этот параметр позволяет указать только одну область.</p>            |
| <путь к TXT-файлу со списком областей мониторинга> | <p>Укажите путь к TXT-файлу, содержащему список областей мониторинга.</p> <p>Файл должен быть в кодировке UTF-8, а путь к каждой области мониторинга необходимо указывать на отдельной строке.</p> |
| <путь к TXT-файлу>                                 | Укажите путь к файлу, в который вы хотите экспортировать данные всех эталонов.                                                                                                                     |
| <идентификатор эталона>                            | <p>Укажите уникальный идентификатор эталона.</p> <p>Чтобы просмотреть идентификатор эталона, используйте параметр /SHOW.</p>                                                                       |
| <существующее название>                            | Укажите название существующей задачи.                                                                                                                                                              |
| <новое название>                                   | Укажите название новой задачи.                                                                                                                                                                     |

## Коды возврата команд

### В этом разделе

|                                                                 |                     |
|-----------------------------------------------------------------|---------------------|
| Коды возврата команд KAVSHELL START и KAVSHELL STOP .....       | <a href="#">725</a> |
| Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical..... | <a href="#">726</a> |
| Коды возврата команды KAVSHELL TASK LOG-INSPECTOR.....          | <a href="#">726</a> |
| Коды возврата команды KAVSHELL TASK.....                        | <a href="#">727</a> |
| Коды возврата команды KAVSHELL RTP .....                        | <a href="#">727</a> |
| Коды возврата команды KAVSHELL UPDATE.....                      | <a href="#">728</a> |
| Коды возврата команды KAVSHELL ROLLBACK .....                   | <a href="#">728</a> |
| Коды возврата команды KAVSHELL LICENSE .....                    | <a href="#">729</a> |
| Коды возврата команды KAVSHELL TRACE .....                      | <a href="#">729</a> |
| Коды возврата команды KAVSHELL FBRESET .....                    | <a href="#">730</a> |
| Коды возврата команды KAVSHELL DUMP .....                       | <a href="#">730</a> |
| Коды возврата команды KAVSHELL IMPORT .....                     | <a href="#">731</a> |
| Коды возврата команды KAVSHELL EXPORT .....                     | <a href="#">731</a> |
| Коды возврата команды KAVSHELL FIM /BASELINE .....              | <a href="#">732</a> |

## Коды возврата команд KAVSHELL START и KAVSHELL STOP

Table 132. Коды возврата команд KAVSHELL START и KAVSHELL STOP

| Код возврата | Описание                                                                                                                                                               |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                                                                             |
| -3           | Ошибка прав доступа                                                                                                                                                    |
| -5           | Неверный синтаксис команды                                                                                                                                             |
| -6           | Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена)                                                                               |
| -7           | Служба не зарегистрирована                                                                                                                                             |
| -8           | Автоматический запуск службы отключен                                                                                                                                  |
| -9           | Неудачная попытка запустить управляемое устройство под другой учетной записью (по умолчанию служба Kaspersky Security работает под учетной записью Локальная система). |
| -99          | Неизвестная ошибка                                                                                                                                                     |

## Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical

Table 133. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical

| Код возврата | Описание                                                       |
|--------------|----------------------------------------------------------------|
| 0            | Операция выполнена успешно (Угроз не обнаружено)               |
| 1            | Операция отменена                                              |
| -2           | Служба не запущена                                             |
| -3           | Ошибка прав доступа                                            |
| -4           | Объект не найден (не найден файл со списком областей проверки) |
| -5           | Неверный синтаксис команды или не определена область проверки  |
| -80          | Зараженных и других обнаруживаемых объектов                    |
| -81          | Возможно зараженных объектов                                   |
| -82          | Обнаружены ошибки обработки                                    |
| -83          | Обнаружены непроверенные объекты                               |
| -84          | Обнаружены поврежденные объекты                                |
| -85          | Не удалось создать журнал выполнения задачи                    |
| -99          | Неизвестная ошибка                                             |
| -301         | Недействительный ключ                                          |

## Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Table 134. Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

| Код возврата | Описание                                                                                 |
|--------------|------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                               |
| -6           | Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена) |
| 402          | Задача уже запущена (для параметра /STATE)                                               |

## Коды возврата команды KAVSHELL TASK

Table 135. Коды возврата команды KAVSHELL TASK

| Код возврата | Описание                                                                                        |
|--------------|-------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                      |
| -2           | Служба не запущена                                                                              |
| -3           | Ошибка прав доступа                                                                             |
| -4           | Объект не найден (задача не найдена)                                                            |
| -5           | Неверный синтаксис команды                                                                      |
| -6           | Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена) |
| -99          | Неизвестная ошибка                                                                              |
| -301         | Недействительный ключ                                                                           |
| 401          | Задача не запущена (для параметра /STATE)                                                       |
| 402          | Задача уже запущена (для параметра /STATE)                                                      |
| 403          | Задача уже приостановлена (для параметра /STATE)                                                |
| -404         | Сбой выполнения операции (изменение состояния задачи привело ее к сбою)                         |

## Коды возврата команды KAVSHELL RTP

Table 136. Коды возврата команды KAVSHELL RTP

| Код возврата | Описание                                                                    |
|--------------|-----------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                  |
| -2           | Служба не запущена                                                          |
| -3           | Ошибка прав доступа                                                         |
| -4           | Объект не найден (не найдена одна или все задачи постоянной защиты сервера) |
| -5           | Неверный синтаксис команды                                                  |
| -6           | Неверная операция (например, задача уже запущена или уже остановлена)       |
| -99          | Неизвестная ошибка                                                          |
| -301         | Недействительный ключ                                                       |

## Коды возврата команды KAVSHELL UPDATE

Table 137. Коды возврата команды KAVSHELL UPDATE

| Код возврата | Описание                                                                                                    |
|--------------|-------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                  |
| 200          | Все объекты актуальны (базы или программные компоненты в актуальном состоянии)                              |
| -2           | Служба не запущена                                                                                          |
| -3           | Ошибка прав доступа                                                                                         |
| -5           | Неверный синтаксис команды                                                                                  |
| -99          | Неизвестная ошибка                                                                                          |
| -206         | Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат                             |
| -209         | Ошибка подключения к источнику обновлений                                                                   |
| -232         | Ошибка аутентификации при подключении к прокси-серверу                                                      |
| -234         | Ошибка подключения к программе Kaspersky Security Center                                                    |
| -235         | Kaspersky Security для Windows Server не прошел проверку подлинности при соединении с источником обновлений |
| -236         | Базы программы повреждены                                                                                   |
| -301         | Недействительный ключ                                                                                       |

## Коды возврата команды KAVSHELL ROLLBACK

Table 138. Коды возврата команды KAVSHELL ROLLBACK

| Код возврата | Описание                       |
|--------------|--------------------------------|
| 0            | Операция выполнена успешно     |
| -2           | Служба не запущена             |
| -3           | Ошибка прав доступа            |
| -99          | Неизвестная ошибка             |
| -221         | Резервная копия баз не найдена |
| -222         | Резервная копия баз повреждена |



## Коды возврата команды KAVSHELL LICENSE

Table 139. Коды возврата команды KAVSHELL LICENSE

| Код возврата | Описание                                      |
|--------------|-----------------------------------------------|
| 0            | Операция выполнена успешно                    |
| -2           | Служба не запущена                            |
| -3           | Недостаточно прав для управления ключами      |
| -4           | Ключ с указанным номером не найден            |
| -5           | Неверный синтаксис команды                    |
| -6           | Неверная операция (ключ уже добавлен)         |
| -99          | Неизвестная ошибка                            |
| -301         | Недействительный ключ                         |
| -303         | Лицензия распространяется на другую программу |

## Коды возврата команды KAVSHELL TRACE

Table 140. Коды возврата команды KAVSHELL TRACE

| Код возврата | Описание                                                                                                                |
|--------------|-------------------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                              |
| -2           | Служба не запущена                                                                                                      |
| -3           | Ошибка прав доступа                                                                                                     |
| -4           | Объект не найден (не найден путь к папке с файлами журнала трассировки)                                                 |
| -5           | Неверный синтаксис команды                                                                                              |
| -6           | Недопустимая операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено) |
| -99          | Неизвестная ошибка                                                                                                      |

## Коды возврата команды KAVSHELL FBRESET

Table 141. Коды возврата команды KAVSHELL FBRESET

| Код возврата | Описание                   |
|--------------|----------------------------|
| 0            | Операция выполнена успешно |
| -99          | Неизвестная ошибка         |

## Коды возврата команды KAVSHELL DUMP

Table 142. Коды возврата команды KAVSHELL DUMP

| Код возврата | Описание                                                                                                   |
|--------------|------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                 |
| -2           | Служба не запущена                                                                                         |
| -3           | Ошибка прав доступа                                                                                        |
| -4           | Объект не найден (не найден путь к папке с файлом дампа; не найден процесс с указанным идентификатором)    |
| -5           | Неверный синтаксис команды                                                                                 |
| -6           | Неверная операция (попытка выполнения команды KAVSHELL DUMP /OFF, если создание файла дампа уже выключено) |
| -99          | Неизвестная ошибка                                                                                         |

## Коды возврата команды KAVSHELL IMPORT

Table 143. Коды возврата команды KAVSHELL IMPORT

| Код возврата | Описание                                                                                                                                                                                                       |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                                                                                                                     |
| -2           | Служба не запущена                                                                                                                                                                                             |
| -3           | Ошибка прав доступа                                                                                                                                                                                            |
| -4           | Объект не найден (не удается найти конфигурационный файл для импорта)                                                                                                                                          |
| -5           | Неверный синтаксис                                                                                                                                                                                             |
| -99          | Неизвестная ошибка                                                                                                                                                                                             |
| 501          | Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Security для Windows Server не импортировала параметры некоторых функциональных компонентов) |
| -502         | Файл импорта отсутствует или имеет неизвестный формат                                                                                                                                                          |
| -503         | Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Security для Windows Server более поздней или несовместимой версии)                                             |

## Коды возврата команды KAVSHELL EXPORT

Table 144. Коды возврата команды KAVSHELL EXPORT

| Код возврата | Описание                                                                                                                                                                                                        |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                                                                                                                                      |
| -2           | Служба не запущена                                                                                                                                                                                              |
| -3           | Ошибка прав доступа                                                                                                                                                                                             |
| -5           | Неверный синтаксис                                                                                                                                                                                              |
| -10          | Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)                                                                                                              |
| -99          | Неизвестная ошибка                                                                                                                                                                                              |
| 501          | Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Security для Windows Server не экспортировала параметры некоторых функциональных компонентов) |

## Коды возврата команды KAVSHELL FIM /BASELINE

Table 145. Коды возврата команды KAVSHELL FIM /BASELINE

| Код возврата | Описание                                                                                           |
|--------------|----------------------------------------------------------------------------------------------------|
| 0            | Операция выполнена успешно                                                                         |
| -2           | Служба не запущена                                                                                 |
| -3           | Ошибка прав доступа                                                                                |
| -4           | Объект не найден (задача не найдена)                                                               |
| -5           | Неверный синтаксис команды                                                                         |
| -6           | Неверная операция (например, эталон был удален)                                                    |
| -10          | Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу) |
| -12          | Неверный пароль                                                                                    |
| -80          | Не соответствует удаленным эталонным объектам                                                      |
| -85          | Не удалось создать журнал выполнения задачи                                                        |
| -99          | Внутренняя ошибка                                                                                  |
| -303         | Недопустимый лицензионный ключ                                                                     |
| -502         | Задача не запущена                                                                                 |
| 200          | Все объекты соответствуют эталону                                                                  |
| 501          | Задача завершена успешно с ошибкой / комментарием                                                  |

# Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## В этом разделе

|                                                            |                     |
|------------------------------------------------------------|---------------------|
| Способы получения технической поддержки .....              | <a href="#">733</a> |
| Получение технической поддержки по телефону .....          | <a href="#">733</a> |
| Техническая поддержка через Kaspersky CompanyAccount ..... | <a href="#">734</a> |
| Использование файла трассировки и скрипта AVZ .....        | <a href="#">734</a> |

## Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

## Получение технической поддержки по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2b>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки ([https://support.kaspersky.ru/support/rules#ru\\_ru](https://support.kaspersky.ru/support/rules#ru_ru)).

## Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Дополнительную информацию о Kaspersky CompanyAccount см. на веб-сайте Службы технической поддержки ([http://support.kaspersky.ru/faq/companyaccount\\_help](http://support.kaspersky.ru/faq/companyaccount_help)).

## Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Security для Windows Server и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять защищаемое устройство

на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки системы.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность обработки и сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

# АО "Лаборатория Касперского"

"Лаборатория Касперского" — известный в мире производитель систем защиты компьютеров от цифровых угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). "Лаборатория Касперского" — наиболее предпочитаемый производитель систем компьютерной защиты для домашних пользователей в России ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" — это международная группа компаний с 38 офисами в 33 стране мира. В компании работает более 3 000 квалифицированных специалистов.

**Продукты.** Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

**Технологии.** Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu и ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

**Достижения.** За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. По итогам испытаний и исследований, проведенных авторитетной австрийской испытательной лабораторией AV-Comparatives в 2014 году, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" — это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей, а количество организаций, являющихся ее клиентами, превышает 270 000.



Сайт "Лаборатории Касперского":

<https://www.kaspersky.ru>

Вирусная энциклопедия:

<https://securelist.ru>

Kaspersky VirusDesk:

<http://virusdesk.kaspersky.ru/> (для проверки подозрительных файлов и веб-сайтов)

Сообщество пользователей "Лаборатории Касперского":

<https://community.kaspersky.com>

# Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache, Kafka – зарегистрированные товарные знаки или товарные знаки The Apache Software Foundation в США и других странах.

Citrix, XenApp и XenDesktop – товарные знаки Citrix Systems, Inc. и/или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Dell и Dell Compellent – товарные знаки Dell, Inc. или дочерних компаний.

Dropbox – товарный знак Dropbox, Inc.

EMC, Celerra, Isilon, OneFS и VNX – зарегистрированные товарные знаки или товарные знаки EMC Corporation в США и/или других странах.

Hitachi – товарный знак Hitachi, Ltd.

IBM и System Storage – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

NetApp и Data ONTAP товарные знаки или зарегистрированные в США и/или других странах товарные знаки NetApp, Inc.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

# Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Table 146. Соответствие терминов

| Термин в документации                                          | Термин в требованиях ФСТЭК                                                                |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| программа                                                      | продукт, объект оценки, программное изделие                                               |
| вирус, программа, представляющая угрозу, вредоносная программа | КВ, компьютерный вирус                                                                    |
| антивирусные базы, базы программы                              | базы данных признаков компьютерных вирусов (БД ПКВ)                                       |
| антивирусная проверка                                          | поиск вирусов                                                                             |
| события                                                        | данные аудита                                                                             |
| администратор                                                  | администратор безопасности, уполномоченный субъект информационной системы, уполномоченный |

# Глоссарий

## А

### Активный ключ

Ключ, используемый в текущий момент для работы программы.

### Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

### Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

### Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

## Р

### Резервное хранилище

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой дезинфекции или удаления.

## Л

### Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

## У

### Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют следующие уровни важности:

- Критическое событие
- Отказ функционирования

- Предупреждение
- Информационное сообщение

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

## Л

### Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

### Маска файла

Представление имени файла с помощью специальных символов. Стандартными специальными символами, используемыми в масках файлов, являются \* и ?, где \* представляет любое количество символов, а ? представляет любой отдельный символ.

## Э

### Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

## П

### Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe и dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

### Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует обрабатывать такие объекты.

## К

### Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, веб-ресурсов и программ.

Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## С

### Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

### Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

## О

### OLE-объект

Объект, прикрепленный к другому файлу или вложенный в другой файл путем использования технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel®, встроенная в документ Microsoft Office Word.

## П

### Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах одной группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться одновременно к каждой программе.

### Статус защиты

Текущий статус защиты, характеризующий степень защищенности компьютера.

## К

### Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

## П

### Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект (на чтение, запись или исполнение) и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю; объекты, содержащие угрозы, или возможно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются или помещаются на карантин).

## У

### Уровень безопасности

Уровень безопасности представляет собой предварительно заданный набор параметров компонентов программы.

### SIEM

Технология, которая обеспечивает анализ событий безопасности, исходящих от различных сетевых устройств и приложений.

### Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

## З

### Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера и Обновление баз программы.

### Параметры задачи

Параметры программы, специфические для каждого типа задач.

## О

### Обновление

Процедура замены/добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".



## у

### Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

# Приложения

## Программные компоненты Kaspersky Security для Windows Server и их коды для службы Windows Installer

По умолчанию файлы \server\ks4ws\_x86(x64).msi устанавливают все программные компоненты Kaspersky Security для Windows Server. Вы можете включить установку данного компонента при выборочной установке программы.

Файлы \client\ks4wstools\_x86(x64).msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приводятся коды программных компонентов Kaspersky Security для Windows Server для службы Windows Installer. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Security для Windows Server из командной строки.

### В этом разделе

|                                                                    |                    |
|--------------------------------------------------------------------|--------------------|
| Программные компоненты Kaspersky Security для Windows Server ..... | <a href="#">30</a> |
| Программные компоненты набора "Средства администрирования" .....   | <a href="#">34</a> |

## Программные компоненты Kaspersky Security для Windows Server

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Security для Windows Server.

Table 147. Описание программных компонентов Kaspersky Security для Windows Server

| Компонент                 | Код     | Выполняет функции                                                                                                                                                                                                                            |
|---------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Основная функциональность | Core    | Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.                                                                                                                                                     |
| Контроль запуска программ | AppCtrl | Этот компонент отслеживает попытки запуска программ пользователями и разрешает или не разрешает запуск программ в соответствии с заданными правилами контроля запуска программ.<br>Компонент реализуется в задаче Контроль запуска программ. |
| Защита трафика            | WebGW   | Этот компонент обрабатывает сетевой трафик, включая трафик, поступающий через почтовые серверы, перехватывает и проверяет объекты, передаваемые по веб-трафику, на наличие известных компьютерных и других угроз на защищаемом сервере.      |

| Компонент                                                               | Код           | Выполняет функции                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Антивирусная защита                                                     | AVProtection  | Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: <ul style="list-style-type: none"> <li>• Проверка по требованию</li> <li>• Постоянная защита файлов</li> </ul>                                                                                                                                                                                                                                        |
| Проверка по требованию                                                  | Ods           | Этот компонент устанавливает системные файлы Kaspersky Security для Windows Server и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого сервера, выполняемая по требованию).<br><br>Если, устанавливая Kaspersky Security для Windows Server из командной строки, вы укажете другие компоненты Kaspersky Security для Windows Server, не указывая компонент Core, компонент Core будет установлен автоматически. |
| Постоянная защита файлов                                                | Oas           | Этот компонент обеспечивает антивирусную проверку файлов на защищаемом сервере при обращении к этим файлам.<br><br>Компонент реализует задачу Постоянная защита файлов.                                                                                                                                                                                                                                                                       |
| Использование Kaspersky Security Network                                | Ksn           | Этот компонент реализует защиту на основе облачных технологий "Лаборатории Касперского".<br><br>Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).                                                                                                                                                                                                                 |
| Мониторинг файловых операций                                            | Fim           | Этот компонент позволяет фиксировать операции производимые над файлами в выбранной области мониторинга.<br><br>Компонент реализуется в задаче Мониторинг файловых операций.                                                                                                                                                                                                                                                                   |
| Защита от эксплойтов                                                    | AntiExploit   | Этот компонент обеспечивает управление параметрами защиты процессов в памяти защищаемого сервера.                                                                                                                                                                                                                                                                                                                                             |
| Модуль интеграции с Агентом администрирования Kaspersky Security Center | AKIntegration | Обеспечивает связь Kaspersky Security для Windows Server с Агентом администрирования Kaspersky Security Center.<br><br>Вы можете установить этот компонент на защищаемом сервере, если вы планируете управлять программой через Kaspersky Security Center.                                                                                                                                                                                    |
| Анализ журналов                                                         | LogInspector  | Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.                                                                                                                                                                                                                                                                                                                             |

| Компонент                                                          | Код             | Выполняет функции                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Защита RPC-подключаемых сетевых хранилищ.                          | RPCProt         | Этот компонент защищает RPC-подключаемые сетевые хранилища (например, сетевые хранилища от NetApp) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.                                                                                                      |
| Защита ICAP-подключаемых сетевых хранилищ.                         | ICAPProt        | Этот компонент защищает ICAP-подключаемые сетевые хранилища (например, EMC Isilon) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.                                                                                                                      |
| Защита от шифрования для NetApp                                    | AntiCryptorNAS  | Этот компонент защищает папки сетевого хранилища от шифрования. Kaspersky Securityfor Windows Server блокирует доступ к папкам доступа для скомпрометированных компьютеров при обнаружении попытки вредоносного шифрования.                                                                            |
| Набор счетчиков производительности программы "Системный монитор"   | PerfMonCounters | Компонент устанавливает набор счетчиков производительности программы "Системный монитор". Эти счетчики позволяют измерять производительность Kaspersky Security для Windows Server и находить возможные узкие места при совместной работе Kaspersky Security для Windows Server с другими программами. |
| Поддержка SNMP-протокола                                           | SnmpSupport     | Компонент публикует счетчики и ловушки Kaspersky Security для Windows Server через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Вы можете установить этот компонент на защищаемом сервере только в случае, если служба Microsoft SNMP установлена на этом компьютере.           |
| Значок Kaspersky Security для Windows Server в области уведомлений | TrayApp         | Компонент отображает значок Kaspersky Security для Windows Server в области уведомлений панели задач защищаемого сервера. Значок Kaspersky Security для Windows Server показывает состояние защиты компьютера, позволяет открыть Консоль программы (если она установлена) и окно <b>О программе</b> .  |
| Утилита командной строки                                           | Shell           | Позволяет управлять Kaspersky Security для Windows Server из командной строки защищаемого компьютера.                                                                                                                                                                                                  |

## Программные компоненты набора "Средства администрирования"

В следующей таблице содержатся коды и описание программных компонентов набора "Средства администрирования".

Table 148. Описание программных компонентов набора "Средства администрирования"

| Компонент                                      | Код       | Функции компонента                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Оснастка Kaspersky Security для Windows Server | MmcSnapin | Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль программы.<br>Если, устанавливая набор "Средства администрирования" из командной строки, вы укажете другие компоненты набора, не указывая компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически. |
| Справка                                        | Справка   | Chm-файл справки; сохраняется в папке с файлами средств администрирования Kaspersky Security для Windows Server. Вы можете открыть файл справки из меню <b>Пуск</b> или клавишей <b>F1</b> при открытом окне Консоли программы.                                                                               |
| Документация                                   | Docs      | Kaspersky Security для Windows Server сохраняет "Руководство администратора", "Руководство пользователя" в формате PDF на защищаемом компьютере. Вы можете открыть Руководство администратора из меню <b>Пуск</b> .                                                                                           |

## Процессы Kaspersky Security для Windows Server

Kaspersky Security для Windows Server запускает процессы, описанные в таблице ниже.

Table 149. Процессы Kaspersky Security для Windows Server

| Имя файла    | Назначение                                                                            |
|--------------|---------------------------------------------------------------------------------------|
| kavfswp.exe  | Рабочий процесс Kaspersky Security для Windows Server                                 |
| kavtray.exe  | Процесс компонента Значок Kaspersky Security для Windows Server в области уведомлений |
| kavshell.exe | Процесс утилиты командной строки                                                      |
| kavfsrcn.exe | Процесс удаленного управления Kaspersky Security для Windows Server.                  |
| kavfs.exe    | Процесс службы Kaspersky Security Service                                             |
| kavfsgt.exe  | Процесс службы управления Kaspersky Security Management Service                       |
| kavfswb.exe  | Процесс службы контроля внешних процессов Kaspersky Security Broker Host              |

## Изменения в системе после установки Kaspersky Security для Windows Server

При установке Kaspersky Security для Windows Server и Консоли программы (набора "Средства администрирования") служба Windows Installer выполняет на сервере следующие изменения:

- создает папки Kaspersky Security для Windows Server на защищаемом сервере и сервере, где установлена Консоль программы;
- регистрирует службы Kaspersky Security для Windows Server;
- создает группу пользователей Kaspersky Security для Windows Server;
- регистрирует ключи Kaspersky Security для Windows Server в системном реестре.

Эти изменения описаны в таблице ниже.

### Папки Kaspersky Security для Windows Server

Table 150. Папки Kaspersky Security для Windows Server на защищаемом компьютере

| Папка                                                                                                                                                                                                                                                                                                                                                                 | Файлы Kaspersky Security для Windows Server                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Папка %Kaspersky Security for Windows Server%; по умолчанию: <ul style="list-style-type: none"> <li>• В Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\</li> <li>• В Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Security for Windows Server\</li> </ul>                        | Исполняемые файлы Kaspersky Security для Windows Server (папка назначения, указанная при установке).                                                                                               |
| Папка %Kaspersky Security for Windows Server%\mibs                                                                                                                                                                                                                                                                                                                    | Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Kaspersky Security для Windows Server по протоколу SNMP.                                               |
| Папка %Kaspersky Security for Windows Server%\x64                                                                                                                                                                                                                                                                                                                     | 64-разрядные версии исполняемых файлов Kaspersky Security для Windows Server (папка создается только при установке Kaspersky Security для Windows Server в Microsoft Windows 64-разрядной версии). |
| <ul style="list-style-type: none"> <li>• %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Data\</li> <li>• %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Settings\</li> <li>• %ALLUSERSPROFILE%\Application Data\Kaspersky Security for Windows Server\10.1\Dskm\</li> </ul> | Служебные файлы Kaspersky Security для Windows Server.                                                                                                                                             |

| Папка                                                                                                            | Файлы Kaspersky Security для Windows Server                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\              | Файлы с параметрами источников обновлений.                                                                                                                                          |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\Distribution\ | Обновления баз и программных модулей, полученные с помощью задачи Копирование обновлений (папка создается при первом получении обновлений с помощью задачи Копирование обновлений). |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\             | Журналы выполнения задач и журнал системного аудита.                                                                                                                                |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Current\       | Набор баз, используемых в текущий момент.                                                                                                                                           |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Backup\        | Резервная копия баз; перезаписывается при каждом обновлении баз.                                                                                                                    |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Temp\          | Временные файлы, создаваемые во время выполнения задач обновления.                                                                                                                  |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\          | Объекты на карантине (папка по умолчанию).                                                                                                                                          |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\              | Объекты в резервном хранилище (папка по умолчанию).                                                                                                                                 |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored             | Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию).                                                                     |

Table 151. Папки, создаваемые при установке Консоли программы

| Папка                                                                                                                                                                                                                                                                                                                                                           | Файлы Kaspersky Security для Windows Server                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <p>Папка %Kaspersky Security для Windows Server%; по умолчанию:</p> <ul style="list-style-type: none"> <li>В Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\</li> <li>в Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\</li> </ul> | <p>Файлы набора «Средства администрирования» (папка назначения, указанная при установке Консоли программы)</p> |

## Службы Kaspersky Security для Windows Server

Службы Kaspersky Security для Windows Server запускаются под системной учетной записью Локальная система (SYSTEM).

Table 152. Службы Kaspersky Security для Windows Server

| Служба                                                 | Назначение                                                                                                                                        |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Служба Kaspersky Security Service (KAVFS)              | Основная служба Kaspersky Security для Windows Server, которая управляет задачами и рабочими процессами Kaspersky Security для Windows Server.    |
| Служба Kaspersky Security Management Service (KAVFSGT) | Служба, предназначенная для управления программой через Консоль программы.                                                                        |
| Служба Kaspersky Security Broker Service (KAVFSWH)     | Служба, выполняющая роль посредника для сообщения параметров защиты внешним агентам защиты, а также для получения данных о событиях безопасности. |

## Группы Kaspersky Security для Windows Server

Table 153. Группы Kaspersky Security для Windows Server

| Группа                 | Назначение                                                                                                                                                                                   |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KAVWSEE Administrators | Группа на защищаемом Server, пользователи которой имеют полный доступ к Службе Kaspersky Security Management Service, а также доступ ко всем функциям Kaspersky Security для Windows Server. |



## Ключи системного реестра

Table 154. Ключи системного реестра

| Ключ                                                                                                                                                                                                                                                                       | Назначение                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]                                                                                                                                                                                                               | Параметры службы Kaspersky Security для Windows Server.                                |
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]                                                                                                                                                                                         | Параметры журнала событий Kaspersky Security для Windows Server (Kaspersky Event Log). |
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]                                                                                                                                                                                                             | Параметры службы управления Kaspersky Security для Windows Server.                     |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance] | Параметры счетчиков производительности.                                                |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\SnmpAgent]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\WSEE\SnmpAgent]                                                  | Параметры компонента "Поддержка SNMP-протокола".                                       |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\CrashDump]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\CrashDump]                                                 | Параметры записи файла дампа.                                                          |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\Trace]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\Trace]                                                         | Параметры журнала трассировки.                                                         |
| [HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\WSEE\SnmpAgent]                                                                                                                                                                                                       | Параметры задач и функций программы.                                                   |
| [HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\WSEE\10.1\Environment]                                                                                                                                                                                                | Параметры распаковки файлов из проверяемых архивов.                                    |

## Параметры установки и удаления и их ключи для службы Windows Installer

В следующих таблицах описаны параметры установки и удаления Kaspersky Security для Windows Server и их значения по умолчанию, указаны ключи для изменения значений параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды msixexec службы Windows Installer при установке Kaspersky Security для Windows Server из командной строки.

Table 155. Параметры установки и их ключи в Windows Installer

| Параметр                                                                                                                                          | Значение по умолчанию                                                                                                                                                                                                                                                                                                        | Ключ Windows Installer и его значения                                                                                         | Описание                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Принятие условий Лицензионного соглашения                                                                                                         | Отклонить условия Лицензионного соглашения                                                                                                                                                                                                                                                                                   | EULA=<значение><br>0 – вы отклоняете условия Лицензионного соглашения.<br>1 – вы принимаете условия Лицензионного соглашения. | Вам нужно принять условия Лицензионного соглашения для установки Kaspersky Security для Windows Server.                             |
| Папка назначения                                                                                                                                  | Kaspersky Security для Windows Servers:<br>%ProgramFiles%\Kaspersky Lab\Kaspersky Security 10,1<br>для Windows Server .1<br>Средства администрирования:<br>%ProgramFiles%\Kaspersky Lab\Kaspersky Security 10,1<br>для Windows Server .1<br>Admins Tools<br>В Microsoft Windows 64-разрядной версии:<br>%ProgramFiles(x86)%. | INSTALLDIR=<полный путь к папке>                                                                                              | Папка, в которой будут сохранены файлы Kaspersky Security для Windows Server при его установке.<br>Вы можете указать другую папку.  |
| Запуск постоянной защиты файлов при запуске Kaspersky Security для Windows Server ( <b>Включить постоянную защиту после установки программы</b> ) | Запустить                                                                                                                                                                                                                                                                                                                    | RUNRTP=<значение><br>1 – запустить;<br>0 – не запускать.                                                                      | Включите этот параметр, чтобы запустить постоянную защиту файлов при запуске Kaspersky Security для Windows Server (рекомендуется). |

| Параметр                                                                                                                                              | Значение по умолчанию | Ключ Windows Installer и его значения                              | Описание                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Исключения из проверки, рекомендуемые корпорацией Microsoft<br><b>(Добавить к исключениям файлы, рекомендованные Microsoft)</b>                       | Исключать             | ADDMSEXCLUSION=<значение><br>1 – исключать;<br>0 – не исключать.   | В задаче Постоянная защита файлов исключает из области защиты объекты на сервера, которые рекомендует исключать корпорация Microsoft.<br>Некоторые программы на сервере могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, к которым эти программы обращаются. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов. |
| Исключения из проверки, рекомендуемые "Лабораторией Касперского"<br><b>(Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского")</b> | Исключать             | ADDKLEXCLUSION=<значение><br>1 – исключать;<br>0 – не исключать.   | В задаче Постоянная защита файлов исключает из области защиты объекты на сервера, которые рекомендует исключать "Лаборатория Касперского".                                                                                                                                                                                                                                                                  |
| Разрешать удаленное подключение к Консоли программы.                                                                                                  | Не разрешать          | ALLOWREMOTECON = <значение><br>1 – разрешать;<br>0 – не разрешать. | По умолчанию удаленное подключение к Консоли программы, установленной на защищенном сервере, не разрешено. Во время установки вы можете разрешить подключение. Kaspersky Security для Windows Server создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.                                                                                                                 |

| Параметр                           | Значение по умолчанию            | Ключ Windows Installer и его значения | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|----------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Путь к файлу ключа ( <b>Ключ</b> ) | Папка комплекта поставки \server | LICENSEKEYPATH=<имя файла ключа>      | <p>По умолчанию программа установки пытается найти файл с расширением .key в папке \server комплекта поставки.</p> <p>Если в папке \server хранится несколько файлов ключа, программа установки выбирает файл ключа с самой поздней датой истечения срока действия.</p> <p>Вы можете предварительно сохранить файл ключа в папке \server или указать другой путь к файлу ключа с помощью параметра <b>Добавление ключа</b>.</p> <p>Вы можете добавить ключ после установки Kaspersky Security для Windows Server с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ программы во время его установки, после установки Kaspersky Security для Windows Server не будет функционировать.</p> |

| Параметр                       | Значение по умолчанию | Ключ Windows Installer и его значения    | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|-----------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Путь к конфигурационному файлу | Не указан             | CONFIGPATH=<имя конфигурационного файла> | <p>Kaspersky Security для Windows Server импортирует параметры из указанного конфигурационного файла, созданного в программе.</p> <p>Kaspersky Security для Windows Server не импортирует из конфигурационного файла пароли, например, пароли учетных записей Запустить задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную.</p> <p>Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.</p> |

| Параметр                                  | Значение по умолчанию | Ключ Windows Installer и его значения                                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------|-----------------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Разрешение сетевых соединений для Консоли | Выключена             | ADDWFEXCLUSION=<br><значение><br>1 – разрешать;<br>0 – не разрешать. | <p>Используйте этот параметр, если вы устанавливаете Kaspersky Security для Windows Server не на защищаемом компьютере. С помощью Консоли, установленной на другом сервере, вы сможете управлять защитой компьютера удаленно.</p> <p>В брандмауэре Microsoft Windows компьютера будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Security для Windows Server kavfsrcn.exe и открыт доступ к программам DCOM.</p> <p>После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу ESS Administrators на сервера и разрешите на нем сетевые соединения для службы Kaspersky Security Managment Service (файл kavfsgt.exe).</p> <p>В можете подробнее прочитать о дополнительной настройке при установке Консоли программы на другом компьютере (см. раздел "Дополнительная настройка после установки Консоли программы на другом компьютере" на стр. <a href="#">51</a>).</p> |

| Параметр                                                               | Значение по умолчанию | Ключ Windows Installer и его значения                                                                                                                                                      | Описание                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Отключение проверки на наличие несовместимого программного обеспечения | Проверка выполняется  | SKIPINCOMPATIBLES<br>W = <значение><br>0 - выполняется проверка на несовместимое программное обеспечение<br>1 - проверка на наличие несовместимого программного обеспечения не выполняется | Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на устройство в фоновом режиме.<br><br>Независимо от значения данного параметра, при установке Kaspersky Security для Windows Server, программа всегда предупреждает о других версиях программы, установленных на этом же устройстве. |

Table 156. Параметры удаления и их ключи в Windows Installer

| Параметр                                                                                          | Значение по умолчанию | Описание, ключи Windows Installer и их значения                                                                                                                       |
|---------------------------------------------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Восстановление содержимого карантина                                                              | Удалить               | RESTOREQTN =<значение><br>0 – удалить содержимое карантина;<br>1 – восстановить содержимое карантина в папку, указанную параметром RESTOREPATH.                       |
| Восстановление содержимого резервного хранилища                                                   | Удалить               | RESTOREBCK =<значение><br>0 – удалить содержимое резервного хранилища;<br>1 – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH. |
| Ввод текущего пароля для подтверждения операции удаления (при активной функции применения пароля) | Не указан             | UNLOCK_PASSWORD=<заданный пароль>                                                                                                                                     |

| Параметр                           | Значение по умолчанию                                                                           | Описание, ключи Windows Installer и их значения                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Папка для восстановленных объектов | %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\Restored | RESTOREPATH=<полный путь к папке><br>Восстановленные объекты будут сохранены в папке, указанной этим параметром:<br>Объекты из карантина будут сохранены во вложенной папке \Quarantine.<br>Объекты из резервного хранилища – во вложенной папке \Backup. |

## Сертифицированное состояние программы: параметры и их значения

В сертифицированной версии программы Kaspersky Endpoint Security допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния программы

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.  
Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Table 157. Параметры и их значения для программы в сертифицированном состоянии

| Название параметра                   | Краткое описание и диапазон значений                     | Значение параметра для программы в сертифицированном состоянии |
|--------------------------------------|----------------------------------------------------------|----------------------------------------------------------------|
| <b>Параметры установки</b>           |                                                          |                                                                |
| Компонент Управление сетевым экраном | Выбор компонентов для установки на защищаемый компьютер. | Не установлен (флажок снят)                                    |
| Компонент Контроль устройств         | Выбор компонентов для установки на защищаемый компьютер. | Не установлен (флажок снят)                                    |
| Защита от сетевых угроз              | Выбор компонентов для установки на защищаемый компьютер. | Не установлен (флажок снят)                                    |
| Компонент Постоянная защита          | Выбор компонентов для установки на защищаемый компьютер. | Установлен (по умолчанию)                                      |
| Компонент Контроль запуска программ  | Выбор компонентов для установки на защищаемый сервер.    | Установлен (по умолчанию)                                      |



| Название параметра                                             | Краткое описание и диапазон значений                                                                                                                                                           | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                             |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Endpoint Agent                                       | Выбор компонентов для установки на защищаемый сервер.                                                                                                                                          | Установлен (по умолчанию не устанавливается)                                                                                                                                                                               |
| Проверка скриптов                                              | Выбор компонентов для установки на защищаемый сервер.                                                                                                                                          | Установлен (по умолчанию не устанавливается)                                                                                                                                                                               |
| Набор счетчиков производительности программы Системный монитор | Выбор компонентов для установки на защищаемый сервер.                                                                                                                                          | Установлен (по умолчанию не устанавливается)                                                                                                                                                                               |
| <b>Настройки прав доступа и функциональных компонентов</b>     |                                                                                                                                                                                                |                                                                                                                                                                                                                            |
| Служба Kaspersky Security                                      | Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Security. <ul style="list-style-type: none"> <li><b>Запущена</b></li> <li><b>Остановлена</b></li> </ul> | Запущена                                                                                                                                                                                                                   |
| <b>Права на управление программой</b>                          | Доступ к функциям Kaspersky Security для Windows Server: <ul style="list-style-type: none"> <li><b>Разрешить</b></li> <li><b>Запретить</b></li> </ul>                                          | Учетные записи пользователей-администраторов безопасности должны быть добавлены в группу KSWs Administrators.<br>Для всех пользователей и групп, кроме KSWs Administrators и SYSTEM, установлены флажки <b>Запретить</b> . |
| <b>Права на управление службой</b>                             | Доступ к функциям службы Kaspersky Security Service: <ul style="list-style-type: none"> <li><b>Разрешить</b></li> <li><b>Запретить</b></li> </ul>                                              | Учетные записи пользователей-администраторов безопасности должны быть добавлены в группу KSWs Administrators.<br>Для всех пользователей и групп, кроме KSWs Administrators и SYSTEM, установлены флажки <b>Запретить</b> . |

| Название параметра                                                | Краткое описание и диапазон значений                                                                                                                                                                                                         | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                           |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Задача Постоянная защита файлов                                   | <p>Антивирусная проверка файлов на защищаемом сервере при обращении к этим файлам.</p> <ul style="list-style-type: none"> <li>• <b>Выполняется</b></li> <li>• <b>Остановлена</b></li> </ul>                                                  | Выполняется                                                                                                                                                                                                              |
| Лицензирование                                                    | Активация программы с помощью ключа.                                                                                                                                                                                                         | Добавлен файл ключа. По окончании срока действия ключа программа выходит из сертифицированного состояния.                                                                                                                |
| Использовать Локальный KSN                                        | Взаимодействие с Глобальным или Локальным KSN, настраиваемое в Kaspersky Security Center.                                                                                                                                                    | Запускать задачу Использование KSN следует только при использовании Локального KSN (флажок <b>Настроить Локальный KSN</b> установлен), в том числе при отсутствии управления программой через Kaspersky Security Center. |
| <b>Параметры задач Постоянная защита / проверка по требованию</b> |                                                                                                                                                                                                                                              |                                                                                                                                                                                                                          |
| <b>Архивы</b>                                                     | <p>Проверка архивов в указанной области защиты в параметрах задачи Постоянной защиты файлов.</p> <ul style="list-style-type: none"> <li>• <b>Применяется</b> (флажок установлен).</li> <li>• <b>Не применяется</b> (флажок снят).</li> </ul> | Применяется (флажок установлен).                                                                                                                                                                                         |
| <b>Загрузочные секторы дисков и MBR</b>                           | <p>Проверять загрузочные секторы и загрузочные надписи на жестких и съемных дисках сервера.</p> <ul style="list-style-type: none"> <li>• <b>Применяется</b> (флажок установлен).</li> <li>• <b>Не применяется</b> (флажок снят).</li> </ul>  | Применяется (флажок установлен).                                                                                                                                                                                         |

| Название параметра                                          | Краткое описание и диапазон значений                                                                                                                                                                                                                                                                                                                               | Значение параметра для программы в сертифицированном состоянии                                                                    |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Область защиты</b>                                       | Папки и файлы находящиеся под защитой задач Постоянная защита и Проверка по требованию. <ul style="list-style-type: none"> <li>Любые локальные и сетевые папки.</li> </ul>                                                                                                                                                                                         | По умолчанию.<br>Исключение папок из области защиты, установленной по умолчанию, ведет к выходу из сертифицируемого состояния.    |
| <b>Пропускать</b> для любого типа объектов                  | Действия при обнаружении объектов: <ul style="list-style-type: none"> <li><b>Лечить</b></li> <li><b>Удалять</b></li> <li><b>Помещать на карантин</b></li> <li><b>Пропускать</b></li> </ul>                                                                                                                                                                         | Не выбрано.<br>При выборе действия <b>Пропускать</b> для любого типа объектов, программа выходит из сертифицированного состояния. |
| <b>Объекты, проверяемые по указанному списку расширений</b> | На закладке <b>Общие</b> , выберите объекты, которые необходимо защищать: <ul style="list-style-type: none"> <li><b>Все объекты;</b></li> <li><b>Объекты, проверяемые по формату;</b></li> <li><b>Объекты, проверяемые по списку расширений, указанному в антивирусных базах;</b></li> <li><b>Объекты, проверяемые по указанному списку расширений.</b></li> </ul> | Флажок снят.<br>Наполнение списка расширений объектов вручную ведет к выходу программы из сертифицированного состояния.           |
| <b>Исключать файлы</b>                                      | Исключение файлов из проверки по имени файла или маске имени файла: <ul style="list-style-type: none"> <li>Применяется (флажок установлен).</li> <li>Не применяется (флажок снят).</li> </ul>                                                                                                                                                                      | Не применяется (Флажок снят).                                                                                                     |
| <b>Не обнаруживать</b>                                      | Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта:                                                                                                                                                                                                                                                                   | Не применяется (Флажок снят).                                                                                                     |

| Название параметра                                                                                              | Краткое описание и диапазон значений                                                                                                                                                                                                                                                                             | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                 | <ul style="list-style-type: none"> <li>Применяется (флажок установлен).</li> <li>Не применяется (флажок снят).</li> </ul>                                                                                                                                                                                        |                                                                                                                                                                                                                                               |
| <b>Использовать эвристический анализатор</b>                                                                    | Применение эвристического анализатора: <ul style="list-style-type: none"> <li>Применяется (флажок установлен).</li> <li>Не применяется (флажок снят).</li> </ul>                                                                                                                                                 | Применяется (флажок установлен).<br>Снятие флажка ведет к выходу программы из сертифицированного состояния.                                                                                                                                   |
| <b>Параметры задач обновления</b>                                                                               |                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                               |
| <b>Серверы обновлений «Лаборатории Касперского»</b> на компьютере-ретрансляторе (Задача Копирование обновлений) | Источник обновлений баз программы: <ul style="list-style-type: none"> <li><b>Сервер администрирования Kaspersky Security Center.</b></li> <li><b>Серверы обновлений «Лаборатории Касперского».</b></li> <li><b>Другие HTTP-, FTP-серверы или сетевые ресурсы.</b></li> </ul>                                     | На компьютере-ретрансляторе выбран вариант <b>Серверы обновлений «Лаборатории Касперского»</b> .<br>Для работы программы в сертифицированной конфигурации, задачи обновления должны осуществляться через один из защищаемых компьютеров сети. |
| <b>Копировать обновления программы</b> (Задача Копирование обновлений)                                          | Укажите условия копирования обновлений программы: <ul style="list-style-type: none"> <li><b>Копировать обновления программы.</b></li> <li><b>Копировать критические обновления модулей программы.</b></li> <li><b>Копировать обновления баз программы и критические обновления модулей программы.</b></li> </ul> | Выбран вариант <b>Копировать обновления программы</b> .<br>Kaspersky Security для Windows Server загружает только обновления баз Kaspersky Security.                                                                                          |

| Название параметра                                                                                                                                                           | Краткое описание и диапазон значений                                                                                                                                                                                                                                                                    | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Другие HTTP-, FTP-серверы или сетевые ресурсы</b> на серверах-ресиверах.                                                                                                  | <p>Источник обновлений баз программы:</p> <ul style="list-style-type: none"> <li>Сервер администрирования Kaspersky Security Center.</li> <li>Серверы обновлений «Лаборатории Касперского».</li> <li>Другие HTTP-, FTP-серверы или сетевые ресурсы.</li> </ul>                                          | <p>На серверах-ресиверах выбран вариант <b>Другие HTTP-, FTP-серверы или сетевые ресурсы</b>.</p> <p>В качестве источника должна быть указана сетевая папка, настроенная в качестве папки локального источника обновлений в задаче Копирование обновлений на компьютере- ретрансляторе.</p> |
| <b>Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны</b> на серверах-ресиверах. (Задача Обновление баз программы) | <p>При выборе источника обновления <b>Другие HTTP-, FTP-серверы или сетевые ресурсы</b>, активируется функция использования серверо обновлений «Лаборатории Касперского».</p> <ul style="list-style-type: none"> <li>Применяется (флажок установлен).</li> <li>Не применяется (флажок снят).</li> </ul> | <p>Не применяется (флажок снят).</p> <p>Обновление через сервера обновлений «Лаборатории Касперского» запрещено.</p>                                                                                                                                                                        |
| <b>Частота запуска</b> задачи Обновление баз программы                                                                                                                       | <p>Промежуток времени, через которое задача осуществляет проверку наличия обновлений:</p> <ul style="list-style-type: none"> <li>Ежечасно</li> <li>Ежесуточно</li> <li>Еженедельно</li> <li>При запуске программы</li> <li>После получения обновлений Сервером администрирования</li> </ul>             | <p><b>Ежечасно</b> (по умолчанию).</p> <p>Снижение частоты запусков задачи, установленного по умолчанию ведет к выходу программы из сертифицированного состояния.</p>                                                                                                                       |

| Название параметра                                                                                                 | Краткое описание и диапазон значений                                                                                                                                                                                                        | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Настройка параметров аудита</b>                                                                                 |                                                                                                                                                                                                                                             |                                                                                                                                                                                                                 |
| События для компонентов постоянной защиты, проверки по требованию, KSN, лицензирования и обновлений баз программы. | Регистрация событий в параметрах журналов. <ul style="list-style-type: none"> <li>Все события</li> <li>Набор событий по умолчанию</li> </ul>                                                                                                | Для компонентов <b>Постоянная защита, Проверка по требованию, Использование KSN, Лицензирование</b> и задачи <b>Обновление баз программы</b> установлены оповещения о событиях по умолчанию.                    |
| <b>Удалять события в журналах выполнения задач старше, чем (сут.)</b>                                              | Очистка журнала выполнения задач через заданный прометужок времени.                                                                                                                                                                         | <b>30 сут.</b> (по умолчанию).<br>Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.                                                               |
| <b>Удалять события в журнале системного аудита старше, чем (сут.)</b>                                              | Очистка журнала системного аудита через заданный прометужок времени.                                                                                                                                                                        | <b>60 сут.</b> (по умолчанию).<br>Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.                                                               |
| <b>Пороги формирования событий</b>                                                                                 | Промежуток времени, через который возникают события: <ul style="list-style-type: none"> <li>Базы программы устарели.</li> <li>Базы программы сильно устарели.</li> <li>Проверка важных областей компьютера давно не выполнялась.</li> </ul> | По умолчанию выставлены следующие значения:<br><b>7 (сут)</b><br><br><b>14 (сут)</b><br><br><b>30 (сут)</b><br>Уменьшение порога формирования событий ведет к выходу программы из сертифицированного состояния. |

| Название параметра                      | Краткое описание и диапазон значений                                                                                                                                                                       | Значение параметра для программы в сертифицированном состоянии                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Настройка сигналов тревоги</b>       |                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Путем запуска исполняемого файла</b> | <p>Способы уведомления администраторов:</p> <ul style="list-style-type: none"> <li>• Средствами службы сообщений;</li> <li>• Путем запуска исполняемого файла;</li> <li>• По электронной почте.</li> </ul> | <p>Флажок <b>Путем запуска исполняемого файла</b> установлен для событий:</p> <ul style="list-style-type: none"> <li>• Обнаружен объект</li> <li>• Объект не вылечен</li> <li>• Объект не удален</li> <li>• Запуск программы запрещен</li> <li>• Запуск программы запрещен по прецеденту</li> <li>• Объект не помещен на карантин</li> <li>• Объект не помещен в резервное хранилище</li> </ul> |
| <b>Данные сигнала тревоги</b>           | Переменные в составе сообщения сигнала тревоги.                                                                                                                                                            | <p>Переменные <b>Тип обнаруженного объекта</b> (%VIRUS_TYPE%), <b>Обнаружено</b> (%VIRUS_NAME%) и <b>Событие</b> (%EVENT_TYPE%) присутствуют в сообщении сигнала тревоги.</p>                                                                                                                                                                                                                   |