

kaspersky

Kaspersky Endpoint Security 11 для Linux

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.1.0.3013

Обозначение документа: 643.46856491.00049-09 90 01

Содержание

Об этом документе	8
Источники информации о программе	9
О программе	11
Требования	12
Аппаратные и программные требования	12
Инсталляционный комплект	14
Указания по эксплуатации	15
Подготовка к установке программы	17
Установка программы	18
Сценарий установки и первоначальной настройки Kaspersky Endpoint Security	18
Установка пакета Kaspersky Endpoint Security	19
Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center	19
Установка Агента администрирования	20
Удаление программы	21
Локальное удаление Kaspersky Endpoint Security	21
Удаление Kaspersky Endpoint Security через Kaspersky Security Center	22
Процедура приемки	23
Подготовка программы к работе	23
Первоначальная настройка Kaspersky Endpoint Security	23
Шаг 1. Выбор языкового стандарта	23
Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности	24
Шаг 3. Принятие Лицензионного соглашения	24
Шаг 4. Принятие Политики конфиденциальности	24
Шаг 5. Участие в Kaspersky Security Network	24
Шаг 6. Настройка графического пользовательского интерфейса	25
Шаг 7. Определение типа перехватчика файловых операций	25
Шаг 8. Настройка источников обновлений	25
Шаг 9. Настройка параметров прокси-сервера	26
Шаг 10. Загрузка антивирусных баз Kaspersky Endpoint Security	26
Шаг 11. Включение автоматического обновления антивирусных баз	27
Шаг 12. Активация программы	27
Автоматический режим первоначальной настройки Kaspersky Endpoint Security	27
Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security	27
Первоначальная настройка параметров Агента администрирования	29
Настройка разрешающих правил в системе SELinux	30
Настройка разрешающих правил в системе AppArmor	32
Сертифицированное состояние программы	33
Проверка работоспособности. Eicar	33

Разделение доступа к функциям программы по пользовательским ролям	36
Просмотр списка пользователей и ролей.....	37
Назначение роли пользователю	37
Отзыв роли у пользователя	37
Лицензирование программы	38
О лицензии	38
О лицензионном ключе	39
О файле ключа	40
О Лицензионном сертификате.....	40
О предоставлении данных	40
Запуск и остановка программы.....	49
Подготовка к запуску программы в операционной системе Astra Linux.....	50
Мониторинг статуса программы	51
Общие параметры Kaspersky Endpoint Security	52
Команды управления параметрами Kaspersky Endpoint Security и задачами	56
Получение общих параметров Kaspersky Endpoint Security	56
Изменение общих параметров Kaspersky Endpoint Security.....	57
Вывод справки о командах Kaspersky Endpoint Security	58
Включение вывода событий	58
Просмотр информации о программе	59
Установка ограничения на использование памяти программой	60
Команды Kaspersky Endpoint Security	60
Экспорт и импорт параметров программы	67
Управление задачами Kaspersky Endpoint Security с помощью командной строки	69
О задачах Kaspersky Endpoint Security	69
Просмотр списка задач Kaspersky Endpoint Security	71
Создание задачи.....	72
Изменение параметров задачи с помощью конфигурационного файла	73
Изменение параметров задачи с помощью командной строки	73
Восстановление заданных по умолчанию параметров задачи из командной строки	74
Запуск и остановка задачи.....	74
Управление областями проверки из командной строки	75
Управление исключенными областями из командной строки	75
Просмотр состояния задачи	76
Настройка расписания задачи	76
Получение параметров расписания задачи	77
Изменение параметров расписания задачи.....	77
Удаление задачи.....	78
Задача Защита от файловых угроз (File_Threat_Protection ID:1)	79
О защите от файловых угроз	79

Особенности проверки символических и жестких ссылок	80
Параметры задачи Защита от файловых угроз	80
Формирование глобальной области исключения	87
Задача антивирусной проверки (Scan_My_Computer ID:2)	89
Об антивирусной проверке	89
Параметры задачи антивирусной проверки	89
Задача выборочной проверки (Scan_File ID:3)	97
О задаче выборочной проверки	97
Параметры задачи выборочной проверки	97
Задача проверки загрузочных секторов (Boot_Scan ID:4)	105
Задача проверки памяти процессов и памяти ядра (Memory_Scan ID:5)	108
Задача обновления (Update ID:6)	110
Об обновлении баз и модулей программы	110
Об источниках обновлений	111
Параметры задач обновления	111
Установка обновления программы вручную	113
Задача Откат обновления баз (Rollback ID:7)	115
Задача Лицензирование (License ID:9)	116
Добавление дополнительного ключа	116
Удаление активного ключа	116
Удаление дополнительного ключа	117
Задача Управление хранилищем (Backup ID:10)	118
О хранилище	118
Параметры задачи Управление хранилищем	118
Просмотр идентификаторов объектов в хранилище	119
О восстановлении объектов из хранилища	119
Восстановление объектов из хранилища	120
Удаление объектов из хранилища	120
Задача Контроль целостности системы (System_Integrity_Monitoring ID:11)	122
О Контроле целостности системы	122
Контроль целостности системы при доступе (OAFIM)	122
Контроль целостности системы по требованию (ODFIM)	123
Параметры задачи Контроль целостности системы при доступе	124
Параметры задачи Контроль целостности системы по требованию	126
Задача Защита от шифрования (AntiCryptor ID:13)	130
О задаче Защита от шифрования	130
О блокировке доступа к недоверенным компьютерам	131
Параметры задачи Защита от шифрования	131
Просмотр списка заблокированных компьютеров	134
Разблокировка заблокированных компьютеров	134

Задача Защита от веб-угроз (Web_Threat_Protection ID: 14)	136
О задаче Защита от веб-угроз	136
Параметры задачи Защита от веб-угроз	137
Задача Проверка съемных дисков (Removable_Drives_Scan ID: 16)	139
О задаче Проверка съемных дисков	139
Параметры задачи Проверка съемных дисков	139
Задача Проверка контейнеров (Container_Scan ID: 18)	141
О задаче Проверка контейнеров	141
Параметры задачи Проверка контейнеров	141
Интеграция с Jenkins	147
Задача Выборочная проверка контейнеров (Container_Scan ID: 19)	150
О задаче Выборочная проверка контейнеров	150
Параметры задачи Выборочная проверка контейнеров	150
Запуск задачи Выборочная проверка контейнеров	157
Задача Анализ поведения (Behavior_Detection ID: 20)	158
Проверка зашифрованных соединений	159
Параметры сети	159
Управление параметрами проверки зашифрованных соединений	161
Участие в Kaspersky Security Network	162
Об участии в Kaspersky Security Network	162
Включение и выключение использования Kaspersky Security Network	163
Проверка подключения к Kaspersky Security Network	164
События и отчеты	165
Об отчетах	165
Включение вывода событий	166
Просмотр журнала событий в командной строке	166
Просмотр событий в Kaspersky Security Center	167
Проверка целостности компонентов программы	168
Управление программой с помощью Kaspersky Security Center	170
Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере	171
Просмотр состояния защиты компьютера	172
Просмотр параметров Kaspersky Endpoint Security	173
Управление политиками	174
Создание политики	174
Изменение параметров политики	175
Управление задачами	175
Создание локальной задачи	177
Создание групповой задачи	177
Создание задачи для набора компьютеров	177
Запуск, остановка, приостановка и возобновление выполнения задачи вручную	178

Изменение параметров локальной задачи	179
Изменение параметров групповой задачи	179
Изменение параметров задачи для набора устройств	180
Проверка соединения с Сервером администрирования вручную. Утилита klnagchk	180
Подключение к Серверу администрирования вручную. Утилита klmover	181
Использование графического пользовательского интерфейса Kaspersky Endpoint Security	183
Локальное включение и выключение графического пользовательского интерфейса	183
Интерфейс программы	184
Значок программы в области уведомлений	184
Главное окно программы	184
Управление задачами и компонентами	185
Запуск и остановка задач проверки	186
Запуск и остановка задач обновления.....	186
Включение и выключение компонентов программы.....	187
Управление участием в Kaspersky Security Network.....	187
Отчеты	188
Принципы работы с отчетами.....	188
Просмотр отчетов	189
Просмотр объектов в хранилище	190
Создание файла трассировки	190
Устранение уязвимостей и установка критических обновлений в программе	192
Действия после сбоя или неустранимой ошибки в работе программы	193
Обращение в Службу технической поддержки	194
Способы получения технической поддержки	194
Техническая поддержка по телефону.....	194
Техническая поддержка через Kaspersky CompanyAccount	195
Содержимое файлов трассировки и их хранение	195
Содержимое файлов дампа и их хранение	196
Соответствие терминов.....	197
Приложения	198
Конфигурационные файлы задачи по умолчанию	198
Правила редактирования конфигурационных файлов Kaspersky Endpoint Security	198
Конфигурационный файл задачи Защита от файловых угроз	199
Конфигурационный файл задачи Антивирусная проверка.....	200
Конфигурационный файл задачи Выборочная проверка	201
Конфигурационный файл задачи Проверка загрузочных секторов	201
Конфигурационный файл задачи Проверка памяти процессов и памяти ядра.....	202
Конфигурационный файл задачи Обновление	202
Конфигурационный файл задачи Управление хранилищем	202
Конфигурационный файл задачи Контроль целостности системы	202

Конфигурационный файл задачи Защита от шифрования.....	202
Конфигурационный файл задачи Защита от веб-угроз	203
Конфигурационный файл задачи Проверка съемных дисков	203
Конфигурационный файл задачи Проверка контейнеров.....	203
Коды возврата командной строки.....	204
Значения параметров программы в сертифицированном состоянии	204
Информация о стороннем коде	207
Уведомления о товарных знаках	208

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security 11 для Linux" (далее также "Kaspersky Endpoint Security", "программа", "Kaspersky Endpoint Security 11.1.0 для Linux").

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 Endpoint Security, а также поддержка организаций, использующих Kaspersky Endpoint Security. Документ адресован техническим специалистам, которые имеют опыт с системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

Источники информации о программе

Вы можете использовать следующие источники для самостоятельного поиска информации о программе Kaspersky Endpoint Security:

- страница Kaspersky Endpoint Security на веб-сайте “Лаборатории Касперского”;
- страница Kaspersky Endpoint Security на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- сообщество пользователей.

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

Страница Kaspersky Endpoint Security на веб-сайте “Лаборатории Касперского”

На странице программы (<http://www.kaspersky.ru/small-to-medium-business-security/endpoint-linux>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице Kaspersky Endpoint Security в Базе знаний (<https://support.kaspersky.ru/kes11linux>) 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, которые относятся не только к Kaspersky Endpoint Security, но и к другим программам “Лаборатории Касперского”. Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят онлайн-справка и файлы контекстной справки интерфейса программы.

В онлайн-справке вы можете найти информацию о настройке и использовании программы.

В контекстной справке вы можете найти информацию об окнах плагина управления Kaspersky Endpoint Security: перечень и описание параметров.

Электронная справка создана для удобства пользователей и не является полноценным эквивалентом настоящего документа.

Сообщество пользователей

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

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

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки “Лаборатории Касперского”.

О программе

Программное изделие Kaspersky Endpoint Security 11 для Linux (далее также “Kaspersky Endpoint Security”, “программа”) представляет собой средство антивирусной защиты типов “Б”, “В”, “Г” и предназначено для применения на серверах и автоматизированных рабочих местах информационных систем, а также на автономных автоматизированных рабочих местах на аппаратной платформе под управлением операционной системы семейства UNIX™.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) БД ПКВ программы;
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы;
- контроль целостности компонентов программы.

В сертифицированной версии программы не поддерживаются следующие функции:

- задача Управление сетевым экраном (Firewall ID:12);
- задача Контроль устройств (Device_Control ID:15);
- задача Защита от сетевых угроз (Network_Threat_Protection ID:17);
- механизм автоматической загрузки обновлений программы.

Несмотря на то, что параметры некоторых из этих функций отображаются в плагине управления Kaspersky Endpoint Security в Kaspersky Security Center, невозможно использовать эти функции и настроить их параметры.

Требования

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

В этом разделе

Аппаратные и программные	12
Инсталляционный комплект.....	14
Указания по эксплуатации	15

Аппаратные и программные требования

Для функционирования программы Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- процессор Core™ 2 Duo 1.86 ГГц;
- 1 ГБ оперативной памяти для 32-разрядной операционной системы, 2 ГБ оперативной памяти для 64-разрядной операционной системы;
- раздел подкачки не менее 1 ГБ;
- 1 ГБ свободного места на жестком диске.

Программные требования:

- Поддерживаемые 32-битные операционные системы:
 - Ubuntu 16.04 LTS, 16.04.1 LTS, 16.04.2 LTS, 16.04.3 LTS, 16.04.4 LTS, 16.04.5 LTS, 16.04.6 LTS;
 - Red Hat® Enterprise Linux® 6.7, 6.8, 6.9, 6.10;
 - CentOS 6.7, 6.8, 6.9, 6.10;
 - Debian GNU / Linux 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12;
 - Debian GNU / Linux 10.1, 10.2, 10.3;
 - Linux Mint 18.2, 18.3;
 - Linux Mint 19, 19.1, 19.2, 19.3;
 - Альт 8 СП Рабочая Станция;
 - Альт 8 СП Сервер;
 - Альт Рабочая Станция 8;
 - Альт Рабочая Станция К 8;
 - Альт Рабочая Станция 9;
 - Альт Сервер 8;
 - Альт Сервер 9;

- Альт Образование 8;
- Альт Образование 9;
- Гослинукс 6.6;
- Операционная система Лотос (редакция для серверов и рабочих станций);
- Mageia 4.
- Поддерживаемые 64-битные операционные системы:
 - Ubuntu 16.04 LTS, 16.04.1 LTS, 16.04.2 LTS, 16.04.3 LTS, 16.04.4 LTS, 16.04.5 LTS, 16.04.6 LTS;
 - Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS;
 - Red Hat® Enterprise Linux® 6.7, 6.8, 6.9, 6.10;
 - Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
 - Red Hat Enterprise Linux 8.0, 8.1;
 - CentOS 6.7, 6.8, 6.9, 6.10;
 - CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
 - CentOS 8.0, 8.1;
 - Debian GNU / Linux 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12;
 - Debian GNU / Linux 10.1, 10.2, 10.3;
 - OracleLinux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8;
 - OracleLinux 8.0, 8.1;
 - SUSE® Linux Enterprise Server 15, 15 SP 1;
 - openSUSE® Leap 15.0, 15.1;
 - Альт 8 СП Рабочая Станция.
 - Альт 8 СП Сервер.
 - Альт Рабочая Станция 8.
 - Альт Рабочая Станция К 8.
 - Альт Рабочая Станция 9.
 - Альт Сервер 8.
 - Альт Сервер 9.
 - Альт Образование 8.
 - Альт Образование 9.
 - Amazon Linux AMI;
 - Linux Mint 18.2, 18.3;
 - Linux Mint 19, 19.1, 19.2, 19.3;
 - Astra Linux Special Edition 1.5;
 - Astra Linux Special Edition 1.6;
 - Astra Linux Common Edition «Орел» 2.12;

- Гослинукс 6.6;
- Гослинукс 7.2;
- Операционная система Лотос (редакция для серверов и рабочих станций);
- РЕД ОС 7.1;
- РЕД ОС 7.2;
- AlterOS 7.5;
- Pardus OS 19.1.
- интерпретатор языка Perl версии 5.10,
- установленная утилита which,
- установленные пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind),
- исходный код ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.

Перед установкой Kaspersky Endpoint Security и Агента администрирования в операционной системе SUSE Linux Enterprise Server 15 SP1 требуется установить пакет insserv-compat.

Для операционных систем Red Hat Enterprise Linux 8.0 и CentOS 8.0 требуется установить пакет perl-Getopt-Long.

Программа Kaspersky Endpoint Security 11.1.0 для Linux совместима с Kaspersky Security Center следующих версий:

- Kaspersky Security Center 10 Service Pack 3,
- Kaspersky Security Center 11,
- Kaspersky Security Center 12.

Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++® 2015 Redistributable Update 3 RC (<https://www.microsoft.com/ru-ru/download/details.aspx?id=52685>).

Инсталляционный комплект

В комплект поставки входит дистрибутив Kaspersky Endpoint Security, содержащий следующие файлы:

- kesi-11.1.0-<номер сборки>.cert.i386.rpm, kesi_11.1.0-<номер сборки>.cert_i386.deb
Содержат основные файлы Kaspersky Endpoint Security. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом пакетного менеджера.
- kesi-11.1.0-<номер сборки>.cert.x86_64.rpm, kesi_11.1.0-<номер сборки>.cert_amd64.deb
Содержат основные файлы Kaspersky Endpoint Security. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом пакетного менеджера.
- kesi-astra_11.1.0-<номер сборки>_amd64.deb
Содержат основные файлы Kaspersky Endpoint Security для установки на операционные системы Astra Linux Special Edition.
- kesi.zip

Содержит файлы, используемые в процедуре удаленной установки Kaspersky Endpoint Security с помощью Kaspersky Security Center.

- klnagent-<номер сборки>.i386.rpm, klnagent_<номер сборки>_i386.deb, klnagent64-<номер сборки>.x86_64.rpm, klnagent64_<номер сборки>_amd64.deb

Содержит Агент администрирования (компонент Kaspersky Security Center, обеспечивающий взаимодействие между Сервером администрирования Kaspersky Security Center и Kaspersky Endpoint Security).

- klnagent-rpm.tar.gz, klnagent-deb.tar.gz

Содержат файлы klnagent.kpd и akinstall.sh, используемые в процедуре удаленной установки Агента Администрирования с помощью Kaspersky Security Center.

- ksn_license.<ID языка>

Содержит текст Положения о Kaspersky Security Network.

- license.<ID языка>

Содержит текст Лицензионного соглашения. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Указания по эксплуатации

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” на стр. [12](#).
3. Перед установкой и эксплуатацией программы на компьютере следует установить все доступные обновления операционной системы.
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 контролируемыми 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. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. 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.

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” на стр. [12](#).

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.

Установка программы

Этот раздел содержит инструкции по установке Kaspersky Endpoint Security из пакета установки (далее “пакет”) и по установке Агента администрирования.

В этой главе

Сценарий установки и первоначальной настройки Kaspersky Endpoint Security	18
Установка пакета Kaspersky Endpoint Security	19
Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center.....	19
Установка Агента администрирования	20

Сценарий установки и первоначальной настройки Kaspersky Endpoint Security

Сценарий описывает установку и первоначальную настройку программы Kaspersky Endpoint Security, а также установку и настройку пакета Агента администрирования.

Установка и первоначальная настройка Kaspersky Endpoint Security и Kaspersky Security Center состоит из следующих этапов:

a. Удаление сторонних антивирусных программ

Перед установкой программы Kaspersky Endpoint Security убедитесь, что на вашем компьютере не установлены другие сторонние антивирусные программы.

b. Установка пакета Kaspersky Endpoint Security

Программа Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security из пакета нужного формата (см. раздел “Установка пакета Kaspersky Endpoint Security” на стр. [19](#)).

c. Первоначальная настройка Kaspersky Endpoint Security

После завершения установки Kaspersky Endpoint Security запустите скрипт послеустановочной настройки (см. раздел “Первоначальная настройка Kaspersky Endpoint Security” на стр. [23](#)). Выполнение первоначальной настройки необходимо для включения защиты вашего компьютера. Скрипт послеустановочной настройки Kaspersky Endpoint Security входит в пакет Kaspersky Endpoint Security (см. раздел “Инсталляционный комплект” на стр. [14](#)).

На этапе первоначальной настройки можно вручную указать значения параметров или использовать конфигурационный файл первоначальной настройки (см. раздел “Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security” на стр. [27](#)) для выполнения первоначальной настройки автоматически (см. раздел “Автоматический режим первоначальной настройки Kaspersky Endpoint Security” на стр. [27](#)). При необходимости можно изменить значения параметров в конфигурационном файле первоначальной настройки.

d. Установка Агента администрирования

Установите Агент администрирования (см. раздел “Установка Агента администрирования” на стр. [20](#)). Этот шаг необходим, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center (см. раздел “Управление программой с помощью Kaspersky Security Center” на стр. [170](#)).

e. Первоначальная настройка Агента администрирования

После установки Агента администрирования настройте его параметры (см. раздел “Первоначальная настройка параметров Агента администрирования” на стр. [20](#)).

f. Установка плагина управления Kaspersky Endpoint Security

Для управления Kaspersky Endpoint Security с помощью Kaspersky Security Center требуется установить плагин управления Kaspersky Endpoint Security. Дополнительная информация приведена в документации Kaspersky Security Center (<https://help.kaspersky.com/KSC/11/ru-RU/6393.htm>).

Во время установки программы или загрузки и применения обновлений программы, требуются root-права для доступа к файлам и директориям программы.

Установка пакета Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kesi-11.1.0-<номер сборки>.cert.i386.rpm
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kesi-11.1.0-< номер сборки>.cert.x86_64.rpm
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# dpkg -i kesi-11.1.0-<номер сборки>.cert_i386.deb
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# dpkg -i kesi_11.1.0-<номер сборки>.cert_amd64.deb
```

- ▶ Чтобы установить Kaspersky Endpoint Security на операционную систему Astra Linux Special Edition, выполните следующую команду:

```
# dpkg -i kesi-astra_11.1.0-<номер сборки>_amd64.deb
```

Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center

Вы можете установить Kaspersky Endpoint Security на компьютер с помощью Kaspersky Security Center.

Подробнее об этом типе установки программы вы можете прочитать в документации для Kaspersky Security Center.

Установка Агента администрирования

Установка Агента администрирования требуется, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Запускать процесс установки Агента администрирования требуется с root-правами.

- ▶ Чтобы установить Агент администрирования из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i klnagent-<номер сборки>.i386.rpm
```

- ▶ Чтобы установить Агент администрирования из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i klnagent64-<номер сборки>.x86_64.rpm
```

- ▶ Чтобы установить Агент администрирования из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# dpkg -i klnagent_<номер сборки>_i386.deb
```

- ▶ Чтобы установить Агент администрирования из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# dpkg -i klnagent64_<номер сборки>_amd64.deb
```

После установки пакета запустите скрипт послеустановочной настройки программы Kaspersky Endpoint Security, выполнив следующую команду:

- для 32-битных операционных систем:

```
/opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

- для 64-битных операционных систем:

```
/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

Удаление программы

Этот раздел содержит инструкции о том, как удалить Kaspersky Endpoint Security локально или через Kaspersky Security Center.

В этой главе

Локальное удаление Kaspersky Endpoint Security.....	21
Удаление Kaspersky Endpoint Security через Kaspersky Security Center.....	22

Локальное удаление Kaspersky Endpoint Security

В процессе удаления программы все задачи Kaspersky Endpoint Security будут остановлены.

- ▶ Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e kesc1
```

- ▶ Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата DEB, выполните следующую команду:

```
# dpkg -r kesc1
```

- ▶ Чтобы удалить Kaspersky Endpoint Security, установленный на операционную систему Astra Linux Special Edition, выполните следующую команду:

```
# dpkg -r kesc1-astra
```

- ▶ Чтобы удалить Агент администрирования, который был установлен на 32-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent
```

- ▶ Чтобы удалить Агент администрирования, который был установлен на 64-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent64
```

- ▶ Чтобы удалить Агент администрирования, который был установлен на 32-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# dpkg -r klnagent
```

- ▶ Чтобы удалить Агент администрирования, который был установлен на 64-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# dpkg -r klnagent64
```

Программа автоматически выполняет процедуру удаления. По завершении программа выводит сообщение о результатах удаления.

После удаления Kaspersky Endpoint Security база данных лицензии сохраняется, и ее можно использовать для повторной установки программы.

Удаление Kaspersky Endpoint Security через Kaspersky Security Center

Вы можете удалить Kaspersky Endpoint Security через Kaspersky Security Center. Для этого вам нужно создать и запустить задачу удаления Kaspersky Endpoint Security.

Подробнее о создании и запуске задачи удаления Kaspersky Endpoint Security вы можете прочитать в документации для Kaspersky Security Center.

Процедура приемки

После успешной установки программы перед ее вводом в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности, подготовку программы к работе и приведение конфигурации программы в соответствие сертифицируемой конфигурации.

В этом разделе

Подготовка программы к работе	23
Сертифицированное состояние программы	33
Проверка работоспособности. Eiscar.....	33

Подготовка программы к работе

Этот раздел содержит инструкции о первоначальной настройке программы Kaspersky Endpoint Security и параметров Агента администрирования.

Первоначальная настройка Kaspersky Endpoint Security

После установки программы Kaspersky Endpoint Security требуется запустить скрипт послеустановочной настройки Kaspersky Endpoint Security. Скрипт послеустановочной настройки Kaspersky Endpoint Security входит в пакет Kaspersky Endpoint Security.

Если вы не выполнили процедуру первоначальной настройки программы Kaspersky Endpoint Security, антивирусная защита компьютера не будет работать.

- Чтобы запустить скрипт послеустановочной настройки Kaspersky Endpoint Security, выполните следующую команду:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Скрипт послеустановочной настройки пошагово запрашивает значения параметров программы Kaspersky Endpoint Security.

Скрипт послеустановочной настройки требуется запускать с root-правами после завершения установки пакета Kaspersky Endpoint Security.

Шаг 1. Выбор языкового стандарта

На этом шаге вам нужно задать обозначение языкового стандарта, который будет использоваться при работе Kaspersky Endpoint Security.

Вы можете задать языковой стандарт в формате, определенном в RFC 3066.

- ▶ Чтобы получить полный список обозначений языковых стандартов, выполните следующую команду:

```
# locale -a
```

По умолчанию программа предлагает использовать языковой стандарт, установленный для root.

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге ознакомьтесь с текстом Лицензионного соглашения, которое заключается между вами и “Лабораторией Касперского”, и Политики конфиденциальности, которая описывает обработку и передачу данных. Для этого нажмите на клавишу Enter. Для завершения просмотра используйте клавишу Q. Файл `license.<ID языка>` с текстом Лицензионного соглашения и Политики конфиденциальности расположен в директории `/opt/kaspersky/kesl/doc/`.

Шаг 3. Принятие Лицензионного соглашения

На этом шаге вам нужно принять или отклонить условия Лицензионного соглашения.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения;
- `no` (или `n`), если вы не согласны с условиями Лицензионного соглашения.

Если вы не согласны с условиями Лицензионного соглашения, программа прерывает процесс настройки Kaspersky Endpoint Security.

Шаг 4. Принятие Политики конфиденциальности

На этом шаге вам нужно принять или отклонить условия Политики конфиденциальности.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете Политику конфиденциальности;
- `no` (или `n`), если вы не принимаете Политику конфиденциальности.

Если вы не согласны с условиями Политики конфиденциальности, программа прерывает процесс настройки Kaspersky Endpoint Security.

Шаг 5. Участие в Kaspersky Security Network

На этом шаге вам нужно принять или отклонить условия Положения о Kaspersky Security Network.

Файл `ksn_license.<ID языка>` с текстом Положения о Kaspersky Security Network находится в директории `/opt/kaspersky/kesl/doc/`.

Введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Положения о Kaspersky Security Network. Будет включен расширенный режим Kaspersky Security Network.
- `no` (или `n`), если вы не принимаете условия Положения о Kaspersky Security Network.

Для сохранения сертифицированной конфигурации программы допустимо использование только Локального KSN (KPSN). В противном случае использование KSN должно быть выключено.

Отказ от участия в Kaspersky Security Network не прерывает процесс установки Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент (см. раздел “Включение и выключение использования Kaspersky Security Network” на стр. [163](#)).

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

Шаг 6. Настройка графического пользовательского интерфейса

На этом шаге можно включить использование графического пользовательского интерфейса (GUI).

Введите одно из следующих значений:

- `yes` (или `y`), чтобы включить использование графического пользовательского интерфейса. Программа Kaspersky Endpoint Security проверит наличие всех нужных библиотек и при необходимости попытается установить отсутствующие.
- `no` (или `n`), чтобы не включать использование графического пользовательского интерфейса.

Вы можете включить или выключить использование графического пользовательского интерфейса в любой момент (см. раздел “Включение и выключение графического пользовательского интерфейса” на стр. [183](#)).

Шаг 7. Определение типа перехватчика файловых операций

На этом этапе определяется тип перехватчика файловых операций для используемой операционной системы. Для операционных систем, не поддерживающих технологию fanotify, будет запущена компиляция модуля ядра.

Если в процессе компиляции модуля ядра не обнаружены необходимые пакеты, Kaspersky Endpoint Security предлагает установить их. Если скачать пакеты не удалось, выводится сообщение об ошибке.

При наличии всех необходимых пакетов модуль ядра будет автоматически скомпилирован при запуске задачи Защита от файловых угроз.

Вы можете выполнить компиляцию модуля ядра позже, после завершения первоначальной настройки программы Kaspersky Endpoint Security.

Шаг 8. Настройка источников обновлений

На этом шаге вам нужно указать источники обновлений баз и модулей программы Kaspersky Endpoint Security.

Введите одно из следующих значений:

- `KLServers` – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений “Лаборатории Касперского”.

- `SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.
- `<Url>` – Kaspersky Endpoint Security загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Шаг 9. Настройка параметров прокси-сервера

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Для загрузки антивирусных баз Kaspersky Endpoint Security с серверов обновлений требуется подключение к интернету (см. раздел “Шаг 10. Загрузка антивирусных баз Kaspersky Endpoint Security” на стр. [26](#)).

► *Чтобы настроить параметры прокси-сервера, выполните одно из следующих действий:*

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
 - `proxy_server_IP:port_number`, если для подключения к прокси-серверу не требуется аутентификация;
 - `user_name:password@proxy_server_IP_address:port_number`, если для подключения к прокси-серверу требуется аутентификация.
- Если для подключения к интернету не используется прокси-сервер, введите значение `no`.

По умолчанию в программе указано значение `no`.

Вы можете настроить параметры прокси-сервера без использования скрипта первоначальной настройки.

Шаг 10. Загрузка антивирусных баз Kaspersky Endpoint Security

На этом шаге вы можете загрузить на компьютер антивирусные базы программы Kaspersky Endpoint Security. Антивирусные базы содержат описания сигнатур угроз и методов борьбы с ними. Kaspersky Endpoint Security использует эти записи при поиске и обезвреживании угроз. Вирусные аналитики “Лаборатории Касперского” регулярно пополняют записи о новых угрозах.

Чтобы загрузить антивирусные базы программы Kaspersky Endpoint Security на компьютер, введите `yes`.

Введите `no`, если вы хотите отказаться от немедленной загрузки антивирусных баз.

По умолчанию предлагается ответ `yes`.

Программа будет обеспечивать антивирусную защиту компьютера только после загрузки антивирусных баз Kaspersky Endpoint Security.

Вы можете запустить задачу обновления без использования скрипта первоначальной настройки.

Шаг 11. Включение автоматического обновления антивирусных баз

На этом шаге вы можете включить автоматическое обновление антивирусных баз.

Введите `yes`, чтобы включить автоматическое обновление антивирусных баз.

По умолчанию Kaspersky Endpoint Security проверяет наличие обновлений для антивирусных баз каждые 60 минут. Если обновления есть, Kaspersky Endpoint Security загружает обновленные антивирусные базы.

Введите `no`, если вы не хотите, чтобы программа Kaspersky Endpoint Security автоматически обновляла антивирусные базы.

Вы можете включить автоматическое обновление антивирусных баз без помощи скрипта первоначальной настройки, настроив расписание задачи обновления (см. раздел “Изменение параметров расписания задачи” на стр. [77](#)).

Шаг 12. Активация программы

На этом шаге вам нужно активировать программу с помощью файла ключа. Для этого требуется указать полный путь к файлу ключа.

Если файл ключа не указан, программа будет активирована с помощью пробного ключа на один месяц.

Вы можете активировать программу без использования скрипта первоначальной настройки (см. раздел “О лицензионном ключе” на стр. [39](#)).

Автоматический режим первоначальной настройки Kaspersky Endpoint Security

Вы можете выполнить первоначальную настройку программы Kaspersky Endpoint Security в автоматическом режиме. Программа установит значения параметров, указанные в конфигурационном файле первоначальной настройки.

- Чтобы запустить первоначальную настройку Kaspersky Endpoint Security в автоматическом режиме, выполните следующую команду:

```
kesl-setup.pl --autoinstall=<полный путь к исходному конфигурационному файлу>
```

Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

Конфигурационный файл первоначальной настройки Kaspersky Endpoint Security содержит параметры, приведенные в таблице ниже.

Таблица 1. Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр Согласие с условиями Лицензионного соглашения	<ul style="list-style-type: none"> • <code>yes</code> – принять условия Лицензионного соглашения, чтобы продолжить процедуру установки программы. • <code>no</code> – не принимать Лицензионное соглашение. Установка программы будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр Принятие Политики конфиденциальности	<ul style="list-style-type: none"> • <code>yes</code> – принять Политику конфиденциальности, чтобы продолжить процедуру установки программы. • <code>no</code> – не принимать Политику конфиденциальности. Установка программы будет прервана.
USE_KSN	Согласие с Положением о Kaspersky Security Network	<ul style="list-style-type: none"> • <code>yes</code> – принять Положение о Kaspersky Security Network. • <code>no</code> – не принимать Положение о Kaspersky Security Network. <p>Для сохранения сертифицированной конфигурации программы допустимо использование только Локального KSN (KPSN). В противном случае использование KSN должно быть выключено.</p>
LOCALE	Дополнительный параметр Языковой стандарт, используемый при работе Kaspersky Endpoint Security	<p>Языковой стандарт в формате, определенном в RFC 3066.</p> <p>Если параметр <code>LOCALE</code> не указан, устанавливается языковой стандарт системы по умолчанию.</p>
INSTALL_LICENSE	Файл ключа	Нет
UPDATER_SOURCE	Источник обновлений	<ul style="list-style-type: none"> • <code>SCServer</code> – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. • <code>KLServers</code> – использовать в качестве источника обновлений серверы “Лаборатории Касперского”. • Адрес источника обновлений
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету	Адрес прокси-сервера.
UPDATE_EXECUTE	Запуск задачи обновления баз во время процедуры настройки	<ul style="list-style-type: none"> • <code>yes</code> – запускать задачу обновления.

		<ul style="list-style-type: none"> • <code>no</code> – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра	<ul style="list-style-type: none"> • <code>yes</code> – компилировать модуль ядра. • <code>no</code> – не компилировать модуль ядра.
USE_GUI	Включение использования графического пользовательского интерфейса	<ul style="list-style-type: none"> • <code>yes</code> – включить использование графического пользовательского интерфейса. • <code>no</code> – выключить использование графического пользовательского интерфейса. <p>Чтобы изменения значений параметров вступили в силу, требуется перезапустить программу.</p>
ADMIN_USER_IF_USE_GUI	Пользователь, которому вы можете назначить роль администратора при включении использования графического пользовательского интерфейса	Нет
IMPORT_SETTINGS	Использование параметров программы из конфигурационного файла	<ul style="list-style-type: none"> • <code>yes</code> – использовать параметры программы из конфигурационного файла. • <code>no</code> – не использовать параметры программы из конфигурационного файла.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security, вводите значения параметров в формате `имя параметра=значение_параметра` (программа не обрабатывает пробелы между именем параметра и его значением).

Первоначальная настройка параметров Агента администрирования

Если вы планируете управлять программой Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно настроить параметры Агента администрирования.

► Чтобы настроить параметры Агента администрирования, выполните следующие действия:

1. Выполните следующую команду:

- для 32-битных операционных систем:

```
# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

- для 64-битных операционных систем:

```
# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

2. Укажите DNS-имя или IP-адрес Сервера администрирования.
3. Укажите номер порта Сервера администрирования.
По умолчанию используется порт 14000.
4. Если вы хотите использовать SSL-соединение, укажите номер SSL-порта Сервера администрирования.
По умолчанию используется порт 13000.
5. Выполните одно из следующих действий:
 - Введите `yes`, чтобы использовать SSL-соединение.
 - Введите `no`, чтобы не использовать SSL-соединение.По умолчанию SSL-соединение включено.
6. При необходимости укажите режим шлюза соединений:
 - 0 – не использовать шлюз соединений.
 - 1 – использовать Агент администрирования в качестве шлюза соединений.
 - 2 – подключаться к Серверу администрирования с помощью шлюза соединений.

Для получения подробной информации о настройке Агента администрирования обратитесь к документации [Kaspersky Security Center](#).

Настройка разрешающих правил в системе SELinux

- Чтобы настроить SELinux для работы с *Kaspersky Endpoint Security*, выполните следующие действия:

1. Переведите SELinux в разрешающий режим:
 - Если SELinux был активирован, выполните следующую команду:

```
# setenforce Permissive
```
 - Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита `semanage utility`. Если утилита не установлена, установите пакет `polyscoreutils-python*`.
3. Установите пакет *Kaspersky Endpoint Security* (см. раздел “Установка пакета *Kaspersky Endpoint Security*” на стр. 19).
После установки пакета назначение метки для исходных исполняемых файлов будет выполнено автоматически.
4. Если вы используете пользовательскую политику SELinux, то есть отличную от заданной по умолчанию `targeted policy`, назначьте метку для следующих исходных исполняемых файлов *Kaspersky Endpoint Security* в соответствии с используемой политикой SELinux:

- `/var/opt/kaspersky/kesl/11.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl`
 - `/var/opt/kaspersky/kesl/11.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/bin/kesl-control`
 - `/var/opt/kaspersky/kesl/11.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl-gui`
 - `/var/opt/kaspersky/kesl/11.1.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/shared/kesl-supervisor`
5. Запустите конфигурационный скрипт Kaspersky Endpoint Security:
- ```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```
6. Запустите следующие задачи:
- задачу Защита от файловых угроз:  

```
kesl-control --start-task 1
```
  - задачу проверки загрузочных секторов:  

```
kesl-control --start-task 4 -W
```
  - задачу проверки памяти процессов и памяти ядра:  

```
kesl-control --start-task 5 -W
```

Рекомендуется запустить все задачи, которые вы планируете запускать при использовании Kaspersky Endpoint Security.

7. Убедитесь, что в файле `audit.log` нет ошибок:
- ```
grep kesl /var/log/audit/audit.log
```
8. Если в файле `audit.log` присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи, которые вы планируете запускать при использовании Kaspersky Endpoint Security.

В случае появления новых `audit`-сообщений, связанных с Kaspersky Endpoint Security, требуется обновить файл модуля правил.

9. Переведите SELinux в принудительный режим:

```
# setenforce Enforcing
```

Если вы используете пользовательскую политику SELinux, то после установки обновлений программы вам нужно вручную назначить метку для исходных исполняемых файлов Kaspersky Endpoint Security (выполните шаги 1, 4, 6, 7 и 8).

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Настройка разрешающих правил в системе AppArmor

► Чтобы обновить профили AppArmor, необходимые для работы Kaspersky Endpoint Security, выполните следующие действия:

1. Убедитесь, что модуль AppArmor загружен с помощью одной из следующих команд командной строки:

- `systemctl status apparmor`
- `/etc/init.d/apparmor status`

2. Создайте профиль Kaspersky Endpoint Security:

- a. В первой консоли выполните команды:

```
cd /etc/apparmor.d
aa-genprof /opt/kaspersky/kesl/libexec/kesl
```

- b. Чтобы создать полный профиль, рекомендуется выполнить все операции, которые вы планируете выполнять при использовании Kaspersky Endpoint Security. Например, запускать задачи на второй консоли:

- задачу Защита от файловых угроз:

```
kesl-control --start-task 1
```

- задачу проверки загрузочных секторов:

```
kesl-control --start-task 4 -W
```

- задачу проверки памяти процессов и памяти ядра:

```
kesl-control --start-task 5 -W
```

- задачу обновления:

```
kesl-control --start-task 6 -W
```

Рекомендуется запустить все задачи, которые вы планируете запускать при использовании Kaspersky Endpoint Security.

- c. В первой консоли нажмите **S**. После завершения сканирования событий нажмите **F**.

После этого будет сформирован профиль Kaspersky Endpoint Security для системы AppArmor в директории `/etc/apparmor.d/`.

Имя файла профиля является уникальным для каждой установки (например, `var.opt.kaspersky.kesl.10.1.1.5960_1537783807.opt.kaspersky.kesl.libexec.kesl`).

Созданный профиль можно определить вручную или с помощью команды:

```
basename /etc/apparmor.d/*kesl*
```

3. Переведите созданный профиль Kaspersky Endpoint Security в режим показа сообщений:

```
aa-complain <имя файла профиля Kaspersky Endpoint Security>
```

4. Через несколько дней работы программы обновите профиль, запустив команду:

```
aa-logprof
```


Укажите разрешения `Allow` или `Glob` на все файлы, которые Kaspersky Endpoint Security использовал в течение этого периода.

5. Переведите профиль Kaspersky Endpoint Security в блокирующий режим:

```
aa-enforce <имя файла профиля Kaspersky Endpoint Security>
```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, требуется обновить файл модуля правил.

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Сертифицированное состояние программы

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

- Проведена первоначальная настройка параметров программы (см. раздел “Подготовка программы к работе” на стр. [23](#)).
- Программа активирована: добавлен лицензионный ключ.
- Антивирусные базы обновлены (см. раздел “Задача обновления (Update ID:6)” на стр. [110](#)).
- Настроена и запущена задача Защита от файловых угроз (см. раздел “Задача Защита от файловых угроз (File_Threat_Protection ID:1)” на стр. [79](#)).
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении (см. раздел “Значения параметров программы в сертифицированном состоянии” на стр. [204](#)).
- В журнале событий отсутствуют следующие ошибки в работе программы:
 - ApplicationStopped – Событие об аварийном завершении работы программы.
 - PolicyNotApplied – Событие о том, что основная политика не применилась.
 - IntegrityCheckFailed – Нарушена целостность файлов или модулей программы.
 - LicenseNotInstalled – Ошибка добавления ключа.
 - LicenseExpired – Истек срок действия лицензии.
 - LicenseRevoked - Ключ успешно удален (при условии, что это единственный ключ и нет действующего дополнительного ключа).
 - AVBasesAreTotallyOutOfDate – Базы программы сильно устарели.
 - AVBasesIntegrityCheckFailed – Нарушена целостность баз программы при условии, что базы программы сильно устарели.

Проверка работоспособности. Eicar

Чтобы проверить работоспособность программы, 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. Вы можете загрузить его со страницы сайта EICAR (http://www.eicar.org/anti_virus_test_file.htm).

Перед сохранением файла в директории на диске компьютера убедитесь, что задача Защита от файловых угроз (File_Threat_Protection ID:1) остановлена.

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел “Подготовка программы к работе” на стр. [23](#)).
- Программа находится в сертифицированном состоянии (см. раздел “Сертифицированное состояние программы” на стр. [33](#)).

Проверка работоспособности программы

1. Выполните первоначальную настройку параметров программы (см. раздел “Подготовка программы к работе” на стр. [23](#)).
2. Убедитесь, что программа активирована и антивирусные базы обновлены. Для этого выполните команду:

```
kesl-control --app-info
```

Ожидаемый результат: программа выводит на экран следующую информацию:

```
Key status : Valid
```

```
Anti-virus databases loaded : Yes
```

```
File Threat Protection : Available and running
```

3. Убедитесь, что запущена задача Защита от файловых угроз (File_Threat_Protection ID:1). Для этого выполните команду:

```
kesl-control --get-task-list
```

Ожидаемый результат: задача Защита от файловых угроз (File_Threat_Protection ID:1) присутствует в списке задач, статус задачи Started.

4. Остановите задачу Защита от файловых угроз, выполнив следующую команду:

```
kesl-control --stop-task 1
```

5. Скачайте EICAR-файл с сайта http://www.eicar.org/anti_virus_test_file.htm в разделе **Download**.

Если вы скачали архив, предварительно распакуйте его в защищаемую область. По умолчанию защищается вся файловая система.

6. Запустите задачу Защита от файловых угроз, выполнив следующую команду:

```
kesl-control --start-task 1
```

7. Попробуйте открыть файл eicar.com, выполнив следующую команду:

```
cat <абсолютный путь к файлу>/eicar.com
```

Ожидаемый результат: программа выдает ошибку о том, что указанный файл отсутствует или доступ к нему запрещен.

8. Убедитесь, что зараженный файл был удален из директории компьютера.
9. Проверьте наличие событий об удалении зараженного файла, выполнив следующую команду:

```
kesl-control -E --query "EventType=='ObjectDeleted'"
```

Разделение доступа к функциям программы по пользовательским ролям

Доступ к функциям программы Kaspersky Endpoint Security предоставляется пользователю в соответствии с его ролью. *Роль* – это набор прав и разрешений на управление программой Kaspersky Endpoint Security.

Роли распределяются на четыре группы пользователей операционной системы:

- *kesladmin* соответствует роли Администратор
- *keslusrer* соответствует роли Пользователь
- *keslaudit* соответствует роли Аудитор
- *nokesl* назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

Когда роль Kaspersky Endpoint Security назначается пользователю системы (см. раздел “Назначение роли пользователю” на стр. [37](#)), этот пользователь добавляется в соответствующую группу ролей (см. таблицу *Роли* ниже). При отзыве у пользователя роли программы пользователь удаляется из соответствующей группы ролей.

В таблице ниже описаны три роли Kaspersky Endpoint Security и их права.

Таблица 2. Роли

Название роли	Роль в программе	Права
Администратор	admin	<ul style="list-style-type: none"> • Управление параметрами всех программ и задач • Управление лицензированием программы • Назначение ролей пользователям • Отзыв ролей у пользователей (администратор не имеет права отозвать роль <i>admin</i> у себя самого) • Просмотр и управление хранилищами пользователей
Пользователь	user	<ul style="list-style-type: none"> • Управление только задачами Scan_File • Запуск и остановка задач обновления • Просмотр отчетов для созданных им/ей задач • Просмотр особых событий, общих для всех пользователей программы
Аудитор	audit	<ul style="list-style-type: none"> • Просмотр параметров программы • Просмотр статуса программы • Просмотр всех задач, их параметров и расписания запуска • Просмотр всех событий • Просмотр всех объектов в хранилище

Просмотр списка пользователей и ролей

- ▶ Чтобы просмотреть список пользователей и их ролей, выполните следующую команду:

```
kesl-control [-U] --get-user-list
```

Назначение роли пользователю

- ▶ Чтобы назначить роль определенному пользователю, выполните следующую команду:

```
kesl-control [-U] --grant-role <роль> <пользователь>
```

Пример:

Назначение роли audit пользователю test15:

```
kesl-control --grant-role audit test15
```

Отзыв роли у пользователя

- ▶ Чтобы отозвать роль у определенного пользователя, выполните следующую команду:

```
kesl-control [-U] --revoke-role <роль> <пользователь>
```

Пример:

Отзыв роли audit у пользователя test15:

```
kesl-control --revoke-role audit test15
```

Лицензирование программы

В этом разделе описаны основные аспекты лицензирования программы.

В этой главе

О лицензии	38
О лицензионном ключе	39
О файле ключа	40
О лицензионном сертификате	39
О предоставлении данных	40

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения. *Лицензионное соглашение* – это юридическое соглашение между вами и АО “Лаборатория Касперского”, в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки программы Kaspersky Endpoint Security.
- Прочитав документ license.<ID языка>. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время первоначальной настройки программы.

Если вы не согласны с условиями Лицензионного соглашения, программа прерывает процесс настройки Kaspersky Endpoint Security.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз программы Kaspersky Endpoint Security). Чтобы продолжить использование программы Kaspersky Endpoint Security в режиме полной функциональности, нужно продлить срок действия коммерческой лицензии. Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

- **Пробная** – бесплатная лицензия, предназначенная для ознакомления с программой.

У пробной лицензии обычно короткий срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции.

Активация программы по пробной лицензии приводит к выходу программы из сертифицированного состояния.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами “Лаборатории Касперского”.

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. *Файл ключа* – это файл с расширением .key, который вам предоставляет “Лаборатория Касперского”. *Код активации* – это уникальная последовательность из двадцати латинских букв и цифр.

Использование кода активации для добавления ключа приводит к выходу программы из сертифицированного состояния.

После добавления в программу лицензионный ключ отображается в интерфейсе программы в виде уникальной алфавитно-числовой последовательности.

Лицензионный ключ может быть заблокирован “Лабораторией Касперского” в случае нарушения условий Лицензионного соглашения. Если лицензионный ключ был заблокирован, для работы программы требуется добавить другой ключ.

Лицензионный ключ может быть активным и дополнительным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В программе не может быть несколько активных лицензионных ключей.

Дополнительный лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только после добавления активного лицензионного ключа.

О файле ключа

Файл ключа – это файл с расширением .key, который вам предоставляет “Лаборатория Касперского”. Файлы ключей предназначены для активации программы путем добавления лицензионного ключа.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения программы Kaspersky Endpoint Security или после заказа пробной версии программы Kaspersky Endpoint Security.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации “Лаборатории Касперского”.

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount. Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на сайте “Лаборатории Касперского” (<https://keyfile.kaspersky.com/ru/>) с помощью имеющегося у вас кода активации.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройств, на которых можно использовать программу с предоставленной лицензией);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или условия лицензии;
- тип лицензии.

О предоставлении данных

Если программа была активирована с использованием кода активации, с целью проверки законности использования программы и получения статистической информации о распространении и использовании продуктов держателя лицензии, вы соглашаетесь передавать в автоматическом режиме следующую информацию: код активации, уникальный идентификатор активации текущей лицензии, время активации лицензии, параметры упаковки подтверждения статуса лицензионного ключа, дату и время создания ключа программы, тип, версию и языковые настройки установленной программы, версию установленных обновлений, идентификатор компьютера и идентификатор установки программы на компьютер, идентификаторы компонентов программы, активных на момент предоставления данных.

Если вы используете серверы обновлений “Лаборатории Касперского” для загрузки обновлений, с целью повышения эффективности процедуры обновления и для получения статистической информации о распространении и использовании продуктов держателя лицензии, вы соглашаетесь в автоматическом режиме предоставлять следующую информацию: версию и языковые настройки установленной программы,

идентификаторы компонентов программы, подлежащие обновлению, идентификатор установки программы на компьютер, тип, версию и разрядность операционной системы.

Также, принимая условия Положения о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию об участии в Kaspersky Security Network:

- идентификаторы выполненных команд;
- идентификатор операции, выполняемой сторонним ПО;
- идентификатор обновления стороннего ПО;
- идентификатор регионального центра активации;
- имя отправителя маркетинговых рассылок, определенное эвристически;
- содержимое фрагментов обрабатываемого объекта;
- уникальный идентификатор журнала действий обрабатываемого объекта;
- дата и время истечения срока действия сертификата;
- дата и время выпуска сертификата;
- версия списка отозванных решений служб программы;
- уникальный идентификатор события;
- дата и время возникновения события;
- идентификатор базы, по которой выполняется категоризация программ;
- идентификатор записи в базе программы;
- тип сработавшей записи в антивирусной базе программы;
- версия записи в базе программы;
- идентификатор сработавшей записи в антивирусной базе программы;
- отметка времени сработавшей записи в антивирусной базе программы;
- тип сработавшей записи в антивирусной базе программы;
- дата и время выпуска баз программы;
- отметка времени выпуска баз программы;
- бинарная маска вариантов запроса DNS;
- тип DNS-запроса;
- атакуемый локальный порт;
- идентификатор устройства;
- версия операционной системы;
- номер сборки операционной системы;
- номер обновления операционной системы;
- версия ядра операционной системы;
- расширенная информация о выпуске операционной системе;
- идентификатор операционной системы;
- идентификатор учетной записи, с правами которой был запущен контролируемый процесс;

- IP-адрес
- уникальный идентификатор экземпляра установки программы на компьютере;
- список сетевых интерфейсов на компьютере;
- метод HTTP-запроса;
- местоположение вставки кода в процесс;
- уникальный идентификатор пользователя в системе правообладателя;
- дата активации лицензии;
- дата окончания срока действия лицензии;
- идентификатор лицензии;
- разрядность операционной системы;
- версия операционной системы, установленной на компьютере пользователя;
- индекс зоны, к которой принадлежит IP-адрес узла;
- идентификатор ключа шифрования в хранилище ключей;
- имя компьютера в сети (доменное имя);
- статус лицензии, используемой программой;
- протокол, используемый для подключения к KSN;
- идентификатор веб-сервиса, к которому обращается программа;
- характеристики шифрования пакета данных, отправляемого в KSN;
- идентификатор пакета данных, отправляемого в KSN;
- внешний IP-адрес;
- локальный IP-адрес;
- MAC-адрес источника сетевой атаки;
- название сетевого протокола, используемого при обнаружении сетевой атаки;
- направление сетевого соединения;
- тип учетной записи пользователя, с правами которой был запущен возможно зараженный объект;
- атрибуты файла обрабатываемого объекта;
- последовательность фрагментов обрабатываемого объекта;
- данные внутреннего журнала, сформированного модулем антивирусной программы для обрабатываемого объекта;
- название источника сертификата;
- публичный ключ сертификата;
- алгоритм вычисления публичного ключа сертификата;
- серийный номер сертификата;
- дата и время подписания объекта;
- имя владельца и параметры сертификата;

- отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования;
- дата и время последнего изменения обрабатываемого объекта;
- дата и время создания обрабатываемого объекта;
- характеристики обнаружения;
- атрибуты обрабатываемого исполняемого файла;
- дата и время создания обрабатываемого исполняемого файла;
- описание обрабатываемого объекта, как указано в свойствах объекта;
- энтропия обрабатываемого файла;
- формат обрабатываемого объекта;
- тип контрольной суммы обрабатываемого объекта;
- размер образа программы;
- результат проверки статуса обрабатываемого объекта в KSN;
- дата и время ссылки на исполняемый файл;
- контрольная сумма (MD5) обрабатываемого объекта;
- название обрабатываемого объекта;
- названия упаковщиков, которые упаковали обрабатываемый объект;
- индикатор, показывающий, является ли обрабатываемый объект PE-файлом;
- значение атрибута характеристик из заголовка PE-файла;
- битовая маска раздела директорий данных в PE-файле;
- размер наложения в PE-файле;
- количество разделов в PE-файле;
- значение атрибута подсистемы из заголовка PE-файла;
- название программы;
- контрольная сумма (MD5) маски, блокирующей веб-сервис;
- контрольная сумма (SHA-256) обрабатываемого объекта;
- информация о том, кто подписал обрабатываемый файл;
- размер обрабатываемого объекта;
- флаг, показывающий, запускается ли программа автоматически при старте системы;
- название обнаруженного вредоносного ПО или легального ПО, которое может использоваться для причинения вреда компьютеру или данным пользователя;
- код типа объекта;
- имя поставщика программы;
- решение программы относительно обрабатываемого объекта;
- версия обрабатываемого объекта;
- дата и время первого запуска обрабатываемого объекта;

- источник решения, принятого относительно обрабатываемого объекта;
- контрольная сумма обрабатываемого объекта;
- название родительской программы;
- уровень целостности обрабатываемого объекта;
- контрольная сумма (MD5) обрабатываемого объекта;
- результат проверки целостности модулей;
- обнаруженные файловые операции над обрабатываемым объектом;
- результат действия над обрабатываемым объектом;
- код файловой операции;
- путь к обрабатываемому объекту;
- код директории;
- системный идентификатор процесса (PID);
- права доступа к обрабатываемому объекту;
- информация о результатах проверки сигнатуры файла;
- путь к файлу источника;
- идентификатор уязвимости;
- класс опасности уязвимости;
- выпуск операционной системы;
- полный пути к файлу родительского процесса, используемому для запуска процесса;
- системный идентификатор родительского процесса (PID);
- аргументы командной строки для процесса;
- контрольная сумма кода активации программы;
- идентификатор программы, полученный из лицензии;
- версия компонента программы;
- данные о лицензии для идентификации группы пользователей компании, которые приобрели лицензию, по комментарию в свойствах лицензионного ключа;
- полная версия программы;
- уникальный идентификатор компьютера;
- идентификатор обновления программы;
- идентификатор программы;
- дата и время установки программы;
- дата активации программы;
- идентификатор лицензии на программу;
- контрольная сумма файла ключа программы;
- идентификатор информационной модели, используемой для предоставления лицензии на программу;

- серийный номер лицензионного ключа программы;
- идентификатор сертификата, используемого для подписи заголовка тикета лицензии на программу;
- дата и время создания тикета лицензии на программу;
- контрольная сумма тикета лицензии на программу;
- версия тикета лицензии на программу;
- версия кода активации программы;
- локализация программы;
- тип уведомления инициировавшего отправку статистики;
- версии операционной системы;
- версия программы;
- идентификатор организации-партнера, через которую был размещен заказ на приобретение лицензии на программу;
- информация об обновлениях программы;
- идентификатор установки ПО (PCID);
- идентификатор ребрэндинга программы;
- название компонента программы;
- статус работы компонента программы;
- идентификатор лицензионной программы;
- состояние работоспособности программы после обновления;
- тип установленной программы;
- индикатор участия в KSN;
- формат данных в запросе к инфраструктуре правообладателя;
- идентификатор тикета текущей лицензии;
- идентификатор компонента программы;
- название созданного / измененного сервиса операционной системы;
- ключ сеанса входа;
- алгоритм шифрования для ключа сеанса входа;
- результат действия программы;
- веб-адрес, с которого был загружен файл, соответствующий процессу;
- ответ DNS-сервера;
- IP-адрес DNS-сервера;
- дата и время прекращения получения статистики;
- код ошибки;
- действия пользователя с элементами интерфейса в окне программы;
- IP-адрес атакующего;

- индикатор обнаружения отладки;
- атрибут обрабатываемого объекта, позволяющий отозвать ложно-положительное решение касательно объекта;
- идентификатор задачи, в которой произошло обнаружение;
- количество подключений к KSN, полученных из кеша;
- количество запросов с ответами в локальной базе запросов;
- количество неудачных подключений к KSN;
- количество неудачных транзакций с KSN;
- распределение по времени отмененных запросов к KSN;
- распределение по времени неудачных подключений к KSN;
- распределение по времени неудачных транзакций с KSN;
- распределение по времени успешных подключений к KSN;
- распределение по времени успешных транзакций с KSN;
- распределение по времени успешных запросов к KSN;
- распределение по времени запросов к KSN истекшим временем ожидания;
- количество новых подключений к KSN;
- количество неудачных запросов к KSN, вызванных ошибкой маршрутизации;
- количество неудачных запросов, вызванных отключением KSN в параметрах программы;
- количество неудачных запросов к KSN; вызванных проблемами с сетью;
- количество успешных подключений к KSN;
- количество успешных транзакций с KSN;
- общее количество запросов к KSN;
- задержка в отправке статистики;
- достоверность обнаружения доступа к фишинговому веб-сервису;
- цель фишинговой атаки;
- вес обнаруженного доступа к фишинговому веб-сервису;
- идентификатор протокола;
- идентификатор операции, выполняемой программой;
- дата и время начала получения статистики;
- дата и время обнаружения ПО компонентом Анализ поведения;
- количество обнаруженных программ в контексте компонента Анализ поведения;
- причина обнаружения ПО компонентом Анализ поведения;
- версия отправляемой статистики;
- технические характеристики применяемых технологий обнаружения;
- 4-байтовый вектор, рассчитываемый по первым 4096-байтам раздела;

- числовая величина частоты, рассчитываемая по первым 4096-байтам раздела;
- нулевая величина частоты, рассчитываемая по первым 4096-байтам раздела;
- версия определенного компилятора;
- свойства и контрольные суммы путей в исполняемом файле;
- версия эмулятора;
- 4-байтовый вектор, рассчитываемый по последним 4096-байтам раздела;
- числовая величина частоты, рассчитываемая по последним 4096-байтам раздела;
- нулевая величина частоты, рассчитываемая по последним 4096-байтам раздела;
- свойства и контрольные суммы путей в исполняемом файле;
- глубина эмуляции;
- тип задачи проверки исполняемых файлов, которая отправляет статистику;
- время хранения обрабатываемого объекта;
- алгоритм вычисления отпечатка цифрового сертификата;
- название компонента;
- отметка времени обновления компонента (обновленная версия);
- отметка времени компонента (локальная версия);
- количество неудачных попыток установки обновлений, совершенных компонентом, выполняющим обновления;
- код категории ошибки;
- количество ошибок установки обновлений, совершенных компонентом, выполняющим обновления;
- отметка времени root-индекса для загружаемых обновлений;
- отметка времени root-индекса для доступных обновлений;
- код ошибки задачи обновлений;
- значение фильтра TARGET в задаче обновления;
- тип задачи обновления;
- версия компонента, выполняющего обновления;
- бинарная маска параметров для обрабатываемых объектов;
- контрольная сумма имени пользователя;
- идентификатор безопасности учетной записи пользователя (SID);
- адрес веб-сервиса, к которому обращается программа (URL, IP-адрес);
- заголовок обрабатываемого http-запроса;
- IPv4-адрес веб-сервиса, к которому обращается программа;
- IPv6-адрес веб-сервиса, к которому обращается программа;
- номер порта;
- веб-адрес источника запроса к веб-сервису (источник ссылки);

- обрабатываемый веб-адрес;
- информация о клиенте, использующем сетевой протокол (пользовательский агент);
- идентификатор зоны безопасности, полученный из потока NTFS.

Полученная информация защищается “Лабораторией Касперского” в соответствии с установленными законом требованиями и действующими правилами “Лаборатории Касперского”. Передача данных осуществляется по защищенному каналу.

Более подробная информация об отправке в “Лабораторию Касперского” статистических данных, полученных во время использования Kaspersky Security Network, их хранении и уничтожении приведена в Лицензионном соглашении, Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте “Лаборатории Касперского” (<https://www.kaspersky.com/products-and-services-privacy-policy>). Файлы license.<ID языка> и ksn_license.<ID языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

Запуск и остановка программы

По умолчанию Kaspersky Endpoint Security запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы). Kaspersky Endpoint Security запускает все служебные задачи, а также пользовательские задачи, в параметрах расписания которых задан режим запуска PS.

Если вы остановите Kaspersky Endpoint Security, все выполняющиеся задачи будут прерваны. После повторного запуска Kaspersky Endpoint Security прерванные пользовательские задачи не будут возобновлены автоматически. Только те пользовательские задачи, в параметрах расписания которых задан режим запуска PS, будут запущены снова.

- ▶ *Чтобы запустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl start kesl
```

- ▶ *Чтобы остановить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl stop kesl
```

- ▶ *Чтобы перезапустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl restart kesl
```

- ▶ *Чтобы запустить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl start
```

- ▶ *Чтобы остановить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl stop
```

- ▶ *Чтобы перезапустить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl restart
```

Подготовка к запуску программы в операционной системе Astra Linux

В этом разделе описаны действия, которые требуется выполнить, чтобы запустить программу в операционной системе Astra Linux Special Edition, запущенной в режиме замкнутой программной среды.

Для Astra Linux Special Edition версии 1.6

1. Укажите следующие параметры в файле `/etc/digisig/digisig_initramfs.conf`:

```
DIGSIG_ELF_MODE=1
```

2. Установите пакет совместимости:

```
apt install astra-digisig-oldkeys
```

3. Создайте директорию для ключа программы:

```
mkdir -p /etc/digisig/keys/legacy/kaspersky/
```

4. Разместите ключ программы (`/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg`) в директории, созданной на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digisig/keys/legacy/kaspersky/
```

5. Обновите диски оперативной памяти:

```
update-initramfs -u -k all
```

Для Astra Linux Special Edition версии 1.5

1. Укажите следующие параметры в файле `/etc/digisig/digisig_initramfs.conf`:

```
DIGSIG_LOAD_KEYS=1
```

```
DIGSIG_ENFORCE=1
```

2. Создайте директорию для ключа программы:

```
mkdir -p /etc/digisig/keys/legacy/kaspersky/
```

3. Разместите ключ программы (`/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg`) в директории, созданной на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digisig/keys/legacy/kaspersky/
```

4. Обновите диски оперативной памяти:

```
sudo update-initramfs -u -k all
```

Работа с графическим пользовательским интерфейсом программы поддерживается для сессий с мандатным разграничением доступа.

Мониторинг статуса программы

Мониторинг статуса программы Kaspersky Endpoint Security выполняется с помощью контрольной службы. Контрольная служба автоматически запускается при запуске программы.

В случае сбоя программы генерируется файл дампа, и программа автоматически перезапускается.

- ▶ *Чтобы вывести статус Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl status kesl
```

- ▶ *Чтобы вывести статус Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl status
```

Общие параметры Kaspersky Endpoint Security

В этом разделе описаны общие параметры программы Kaspersky Endpoint Security.

Общие параметры конфигурационного файла имеют следующие значения:

SambaConfigPath

Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере.

После изменения значения этого параметра требуется перезапустить программу.

Значение по умолчанию: `/etc/samba/smb.conf`

NfsExportPath

Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере.

После изменения значения этого параметра требуется перезапустить программу.

Значение по умолчанию: `/etc/exports`

TraceFolder

Директория, в которой хранятся файлы трассировки программы. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел “Содержимое файлов трассировки и их хранение” на стр. [195](#)).

Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security. Для доступа к заданной по умолчанию директории хранения файлов трассировки требуются `root`-права.

После изменения значения этого параметра требуется перезапустить программу.

Значение по умолчанию: `/var/log/kaspersky/kesl`

TraceLevel

Уровень детализации журнала трассировки.

Доступные значения:

`Detailed` – наиболее детализированный журнал трассировки.

`NotDetailed` – журнал трассировки содержит оповещения об ошибках.

`None` – не создает журнал трассировки.

Значение по умолчанию: `None`.

TraceMaxFileCount

Максимальное количество файлов трассировки программы.

Файлы трассировки для текущего и для завершенных процессов трассировки считаются отдельно. Например, если для параметра `TraceMaxFileCount` указано значение 2, то максимально может храниться 4 файла трассировки: два файла для текущего процесса трассировки и два файла для завершенных процессов.

После изменения значения этого параметра требуется перезапустить программу.

Возможные значения: 1 – 10000.

Значение по умолчанию: 5.

TraceMaxFileSize

Максимальный размер файла трассировки программы (в мегабайтах).

После изменения значения этого параметра требуется перезапустить программу.

Возможные значения: 1 – 1000.

Значение по умолчанию: 500.

BlockFilesGreaterMaxFilePath

Блокировка доступа к файлам, длина полного пути к которым превышает заданное значение параметра, в байтах.

Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи антивирусной проверки пропускают такой файл при проверке.

Этот параметр недоступен для операционных систем, в которых используется технологи fanotify.

Возможные значения: 4096 – 33554432.

Значение по умолчанию: 16384.

DetectOtherObjects

Включает или выключает обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Доступные значения:

`Yes` – включить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

`No` – выключить обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Значение по умолчанию: `No`.

NamespaceMonitoring

Включает или отключает проверку пространств имен и Docker-контейнеров.

Доступные значения:

`Yes` – включить проверку пространств имен и Docker-контейнеров.

`No` – выключить проверку пространств имен и Docker-контейнеров.

Значение по умолчанию: `Yes`.

DockerSocket

Адрес файла или сетевого Docker-сокета.

Значение по умолчанию: `/var/run/docker.sock`.

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта. Действия над зараженным объектом *внутри Docker-контейнера* описаны в параметрах соответствующей задачи.

Доступные значения:

`StopContainerIfFailed` – остановить Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – остановить Docker-контейнер при обнаружении зараженного объекта.

`Skip` – не выполнять никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`.

InterceptorProtectionMode

Показывает, блокирует ли программа файлы при проверке.

Доступные значения:

`Full` – блокировать файлы при проверке.

`Info` – не блокировать файлы при проверке, при обнаружении зараженного объекта фиксировать события в журнале событий.

Значение по умолчанию: `Full`.

UseKSN

Включает или выключает участие в Kaspersky Security Network.

Доступные значения:

`No` – выключить участие в Kaspersky Security Network.

`Basic` – включить участие в Kaspersky Security Network без отправки статистики.

`Extended` – включить участие в Kaspersky Security Network с отправкой статистики.

Значение по умолчанию: `No`.

UseProxy

Включает или выключает использование прокси для Kaspersky Security Network, активации программы и обновлений.

Доступные значения:

`Yes` – включить использование прокси.

`No` – выключить использование прокси.

Значение по умолчанию: `No`.

ProxyServer

Параметры прокси-сервера в формате `[пользователь[:пароль]@]узел[:порт]`.

MaxEventsNumber

Максимальное количество событий, которые будет хранить программа Kaspersky Endpoint Security. При превышении заданного количества событий программа удаляет наиболее давние события.

Значение по умолчанию: 500000.

LimitNumberOfScanFileTasks

Максимальное количество задач типа `Scan_File`, которые непривилегированный пользователь может запустить на компьютере одновременно. Этот параметр не ограничивает количество задач, которые запускает пользователь с `root`-правами. Если задано значение 0, непривилегированный пользователь не может запускать задачи типа `Scan_File`.

Возможные значения: 0 – 4294967295.

Значение по умолчанию: 0.

Если во время установки программы для параметра `USE_GUI` установлено значение `yes`, для параметра `LimitNumberOfScanFileTasks` по умолчанию используется значение 5.

UseSyslog

Включает или выключает запись информации о событиях в `syslog`.

Для доступа к `syslog` требуются `root`-права.

Доступные значения:

`Yes` – включить запись информации о событиях в `syslog`.

`No` – выключить запись информации о событиях в `syslog`.

Значение по умолчанию: `No`.

EventsStoragePath

Файл базы данных, в которой Kaspersky Endpoint Security сохраняет информацию о событиях.

Для доступа к заданной по умолчанию базе данных событий требуются `root`-права.

Значение по умолчанию: `/var/opt/kaspersky/kesl/private/storage/events.db`

ExcludedMountPoint.item_#

Точка монтирования, которую требуется исключить из области проверки для задач, использующих перехват файловых операций (Защита от файловых угроз и Защита от шифрования). Вы можете указать несколько точек монтирования, которые требуется исключить из проверки.

Доступные значения:

`AllRemoteMounted` – исключить из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов `SMB` и `NFS`.

`Mounted:NFS` – исключить из проверки все удаленные директории, смонтированные на компьютере с помощью протокола `NFS`.

`Mounted:SMB` – исключить из проверки все удаленные директории, смонтированные на компьютере с помощью протокола `SMB`.

`/mnt` – исключить из проверки объекты, находящиеся в директории `/mnt` (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков.

<путь с применением маски /mnt/user* или /mnt/**/user_share> – исключать из проверки объекты, находящиеся в директориях, имена которых содержат указанную маску.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir*/file или /dir/**/file. Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir**/file/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

Точки монтирования требуется указывать точно так же, как они отображаются в выходных данных команды mount.

Параметр `ExcludedMountPoint.item_#` не указан по умолчанию.

В этой главе

Команды управления параметрами Kaspersky Endpoint Security и задачами	56
Вывод справки о командах Kaspersky Endpoint Security	58
Включение вывода событий	58
Просмотр информации о программе	59
Установка ограничения на использование памяти программой	60
Команды Kaspersky Endpoint Security	60
Экспорт и импорт параметров программы	66

Команды управления параметрами Kaspersky Endpoint Security и задачами

Этот раздел содержит информацию о командах управления параметрами Kaspersky Endpoint Security и задачами.

Получение общих параметров Kaspersky Endpoint Security

Команда `kesl-control --get-app-settings` выводит общие параметры Kaspersky Endpoint Security. Используя эту команду, вы также можете получить общие параметры Kaspersky Endpoint Security, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения общих параметров программы Kaspersky Endpoint Security, установленной на компьютере:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.

3. Импортируйте параметры из конфигурационного файла в программу Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security.

Вы можете использовать созданный конфигурационный файл для импорта параметров в программу Kaspersky Endpoint Security, установленную на другом компьютере.

Синтаксис команды

```
kesl-control [-T] --get-app-settings [--file <имя конфигурационного файла>]
```

Аргументы и ключи

`--file <имя конфигурационного файла>` – имя конфигурационного файла, в котором будут сохранены параметры Kaspersky Endpoint Security. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Пример:

Экспортировать общие параметры программы Kaspersky Endpoint Security в файл с именем `kesl_config.ini`. Сохранить созданный файл в текущей директории:

```
kesl-control --get-app-settings --file kesl_config.ini
```

Изменение общих параметров Kaspersky Endpoint Security

Команда `kesl-control --set-app-settings` устанавливает с помощью ключей команды или импортирует из указанного конфигурационного файла общие параметры Kaspersky Endpoint Security.

Для изменения параметров программы требуется наличие root-прав.

Вы можете использовать эту команду для изменения общих параметров Kaspersky Endpoint Security:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после перезагрузки (см. раздел “Запуск и остановка программы” на стр. [49](#)).

Синтаксис команды

```
kesl-control [-T] --set-app-settings --file <имя конфигурационного файла>
```

```
kesl-control [-T] --set-app-settings <название параметра>=<значение параметра>  
<название параметра>=<значение параметра>
```

Аргументы и ключи

`--file <имя конфигурационного файла>` – имя конфигурационного файла, параметры из которого будут импортированы в Kaspersky Endpoint Security; включает полный путь к файлу.

Примеры:

Импортировать в Kaspersky Endpoint Security общие параметры из конфигурационного файла с именем /home/test/kesl_config.ini:

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Установить низкий уровень детализации журнала трассировки:

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Добавить точку монтирования, которую требуется исключить из области проверки для задач, использующих перехват файловых операций (Защита от файловых угроз и Защита от шифрования):

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Вывод справки о командах Kaspersky Endpoint Security

Команда `kesl-control` с ключом `--help` <набор команд Kaspersky Endpoint Security> возвращает справку по командам Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control --help [<набор команд Kaspersky Endpoint Security>]
```

<набор команд Kaspersky Endpoint Security>

Доступные значения:

- [-T] – команды для управления задачами и общими параметрами Kaspersky Endpoint Security.
- [-L] – команды управления ключами.
- [-B] – команды управления хранилищем.
- [-E] – команды управления событиями Kaspersky Endpoint Security.
- [-F] – команды управления задачей Управление сетевым экраном.

В сертифицированной версии программы задача Управление сетевым экраном недоступна.

- [-H] – команды управления задачей Защита от шифрования.
- [-S] – команды статистики.
- W – мониторинг событий.

Включение вывода событий

Команда `kesl-control -W` включает вывод событий Kaspersky Endpoint Security. Эту команду можно использовать либо отдельно для вывода всех событий безопасности Kaspersky Endpoint Security, либо совместно с командой `kesl-control --start-task` для вывода событий, связанных только с запущенной задачей. Чтобы указать условия для вывода только определенных событий, вы можете использовать команду `--query` с флагом `-W`.

Команда возвращает название события и дополнительную информацию о событии.

Синтаксис команды

```
kesl-control -W
```

Пример:

Включить режим вывода событий Kaspersky Endpoint Security:

```
kesl-control -W
```

Просмотр информации о программе

Команда `kesl-control --app-info` выводит информацию о Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control [-S] --app-info
```

Результат выполнения команды

- **Название.** Название программы.
- **Версия.** Текущая версия программы.
- **Статус ключа.** Статус лицензионного ключа.
- **Статус подписки.** Статус подписки. Это поле отображается, если программа используется по подписке.
- **Дата окончания срока действия лицензии.** Дата окончания срока действия лицензии.
- **Состояние хранилища.** Состояние хранилища. Отображает информацию об ограничениях времени и размера.
- **Использование хранилища.** Размер хранилища.
- **Дата последнего запуска задачи Scan_My_Computer.** Время последнего запуска задачи Scan_My_Computer.
- **Дата последнего выпуска баз.** Время последнего выпуска баз.
- **Антивирусные базы загружены.** Показывает, загружены ли антивирусные базы.
- **Состояние KSN.** Состояние участия в Kaspersky Security Network.
- **Политика.** Показывает, применяется ли политика Kaspersky Security Center или Linux Management Console.
- **Контроль файлов.** Состояние задачи Защита от файловых угроз.
- **Контроль целостности.** Состояние задачи Контроль целостности системы.
- **Управление сетевым экраном.** Состояние задачи Управление сетевым экраном.
- **Защита от шифрования.** Состояние задачи Защита от шифрования.
- **Защита от веб-угроз.** Состояние задачи Защита от веб-угроз.
- **Контроль устройств.** Состояние задачи Контроль устройств.

- **Проверка съемных дисков.** Состояние задачи Проверка съемных дисков.
- **Защита от сетевых угроз.** Состояние задачи Защита от сетевых угроз.
- **Анализ поведения.** Состояние задачи Анализ поведения.
- **Состояние обновления программы.** Показывает действия по обновлению программы и действия, которые должен выполнить пользователь.

В сертифицированной версии программы задачи Управление сетевым экраном, Контроль устройств и Защита от сетевых угроз недоступны.

Установка ограничения на использование памяти программой

Вы можете задать ограничение на использование памяти программой Kaspersky Endpoint Security во время выполнения задач антивирусной проверки (для типов ODS и OAS), в мегабайтах. Минимальное значение: 2048 МБ. Значение по умолчанию: 8192 МБ. Если указанное значение меньше 2048 МБ, программа будет использовать минимальное значение (2048 МБ).

Если указанное значение превышает размер оперативной памяти, будет использоваться до 40% оперативной памяти. Это процентное значение изменить невозможно.

► Чтобы указать ограничение на использование памяти, выполните следующие действия:

1. Остановите Kaspersky Endpoint Security (см. стр. [49](#)).
2. В файле `/var/opt/kaspersky/kesl/common/kesl.ini` добавьте следующий параметр в раздел [General]:
`ScanMemoryLimit=<ограничение на использование памяти в мегабайтах>`
3. Запустите Kaspersky Endpoint Security (см. стр. [49](#)).

Ограничение на использование памяти изменяется при запуске программы.

Команды Kaspersky Endpoint Security

Вы можете менять значения параметров программы Kaspersky Endpoint Security из командной строки.

Ниже приведены правила использования команд Kaspersky Endpoint Security:

- Команды чувствительны к регистру.
- Ключи требуется разделять символом “пробел”.
- При использовании полного названия команды или ключа, требуется указывать значение после символа “равно” (=).

Пример:

Указать значение параметра URL для пользовательского источника обновлений для задачи обновления (ID=6) из командной строки:

```
kesl-control --set-settings 6
```

```
SourceType=Custom CustomSources.item_0000.URL=http://site.domain/path  
CustomSources.item_0000.Enabled=Yes
```

Вывод справки о командах Kaspersky Endpoint Security

```
--help
```

Выводит справку о командах Kaspersky Endpoint Security.

Вывод событий Kaspersky Endpoint Security

```
-W
```

Включает вывод событий Kaspersky Endpoint Security.

Команды управления параметрами Kaspersky Endpoint Security и задачами

```
-T
```

Префикс указывает на то, что команда принадлежит к группе команд управления параметрами Kaspersky Endpoint Security / управления задачами (необязательный).

```
[-S] --app-info
```

Выводит общую информацию о Kaspersky Endpoint Security.

```
[-T] --get-app-settings --file <имя и директория файла>
```

Возвращает общие параметры Kaspersky Endpoint Security.

```
[-T] --set-app-settings --file <имя и директория файла>
```

Устанавливает общие параметры Kaspersky Endpoint Security.

```
[-T] --get-task-list
```

Возвращает список существующих задач Kaspersky Endpoint Security.

```
[-T] --get-task-state <ID задачи>|<имя задачи>
```

Выводит состояние указанной задачи.

```
[-T] --create-task <имя задачи> --type <тип задачи> --file <имя и директория файла>
```

Создает задачу указанного типа, импортирует в задачу параметры из указанного конфигурационного файла.

```
[-T] --delete-task <ID задачи>|<имя задачи>
```

Удаляет задачу.

```
[-T] --start-task <ID задачи>|<имя задачи> [-W] [--progress] [--file <имя и директория файла>]
```

Запускает задачу.

```
[-T] --stop-task <ID задачи>|<имя задачи>
```

Останавливает задачу.

```
[-T] --suspend-task <ID задачи>|<имя задачи>
```

Приостанавливает задачу. Приостановить задачу обновления невозможно.

```
[-T] --resume-task <ID задачи>|<имя задачи>
```

Возобновляет задачу. Возобновить задачу обновления невозможно.

```
[-T] --get-settings <ID задачи>|<имя задачи> --file <имя и директория файла>
```

Выводит параметры задачи.

```
[-T] --set-settings <ID задачи>|<имя задачи> [<параметры>] [--file <имя и директория файла>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <исключение>] [--del-exclusion <исключение>] -set-to-default
```

Устанавливает параметры задачи.

```
[-T] --scan-file <путь> [--action <действие>]
```

Создает и запускает временную задачу Scan_File.

```
[-T] --import-settings --file <полный путь к конфигурационному файлу>
```

Импортирует параметры программы в конфигурационный файл.

```
[-T] --update-application
```

Обновляет программу.

```
[-T] --set-settings {<ID задачи>|<имя задачи>} set-to-default
```

Восстанавливает значения по умолчанию для параметров задачи.

```
[-S] --omsinfo --file <путь>
```

Создает файл в формате JSON для интеграции с Microsoft Operations Management Suite.

Команды управления ключами

```
-L
```

Префикс указывает на то, что команда принадлежит к группе команд управления ключами.

```
[-L] --install-active-key <файл ключа>
```

Добавляет активный ключ.

```
[-L] --install-additional-key <файл ключа>
```

Добавляет дополнительный ключ.

```
[-L] --revoke-active-key
```

Удаляет активный ключ.

```
[-L] --revoke-additional-key
```

Удаляет дополнительный ключ.

```
[-L] --query
```

Выводит информацию о ключе.

Команды для задачи Управление сетевым экраном

```
[-F] --add-rule [--name <строка>] [--action <действие>] [--protocol <протокол>] [--direction <директория>] [--remote <удаленная>] [--local <локальная>] [--at <индекс>]
```

Добавляет новое правило.

```
[-F] --del-rule [--name <строка>] [--index <индекс>]
```

Удаляет правило.

```
[-F] --move-rule [--name <строка>] [--index <индекс>] [--at <индекс>]
```

Изменяет приоритетность правила.

```
[-F] --add-zone [--zone <зона>] [--address <адрес>]
```

Добавляет в зону IP-адрес.

```
[-F] --del-zone [--zone <зона>] [--address <адрес>] [--index <индекс>]
```

Удаляет из зоны IP-адрес.

```
-F --query
```

Отображает информацию.

В сертифицированной версии программы задача Управление сетевым экраном недоступна.

Команды для задачи Защита от шифрования

```
[-H] --get-blocked-hosts
```

Отображает список заблокированных компьютеров.

```
[-H] --allow-hosts
```

Разблокирует недоверенные компьютеры.

Команда для задачи Проверка контейнеров

```
[-T] --scan-container <контейнер|образ[:тег]>
```

Создает временную задачу Проверка контейнеров с параметрами задачи Выборочная проверка контейнеров (идентификатор задачи: 19). После завершения проверки временная задача автоматически удаляется. Вы можете указать имена или маски имен контейнеров и образов. Вы можете также указать идентификаторы контейнеров и образов.

Команды управления пользователями и ролями

```
[-U] --get-user-list
```

Выводит список пользователей и ролей.

```
[-U] --grant-role <роль> <пользователь>
```

Присваивает роль определенному пользователю.

```
[-U] --revoke-role <роль> <пользователь>
```

Отзывает роль у определенного пользователя.

Команды управления хранилищем

-B

Префикс указывает на то, что команда принадлежит к группе команд управления хранилищем.

```
[-B] --mass-remove --query
```

Очищает хранилище, полностью или выборочно.

```
[-B] --query --limit --offset
```

Выводит информацию об объектах в хранилище.

```
--limit
```

Максимальное количество объектов, о которых выводится информация.

```
--offset
```

Количество записей, на которое следует отступить от начала выборки.

```
[-B] --restore <ID объекта> --file <имя и директория файла>
```

Восстанавливает объект из хранилища.

Команды управления журналом событий

-E

Префикс указывает на то, что команда принадлежит к группе команд управления журналом событий.

```
[-E] --query --limit --offset --file <имя и директория файла> --db <файл БД>
```

Максимальное количество событий, о которых выводится информация.

```
--query
```

Выводит информацию о событиях по фильтру из журнала событий или указанного файла ротации.

```
--offset
```

Количество записей, на которое следует отступить от начала выборки.

```
--db
```

Имя файла базы данных.

Команды управления расписанием задач

```
[-T] --set-schedule <ID задачи>|<имя задачи> --file <имя и директория файла>
```

Устанавливает параметры расписания задачи или импортирует их в задачу из конфигурационного файла.

```
[-T] --get-schedule <ID задачи>|<имя задачи> --file <имя и директория файла>
```

Выводит параметры расписания задачи.

```
RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR
```

Расписание запуска задачи.

PS – запускать задачу после запуска программы Kaspersky Endpoint Security.

BR – запускать задачу после обновления антивирусных баз.

```
StartTime=[year/month/month_day] [hh]:[mm]:[ss]; [<month_day>|<week_day>];  
[<period>]
```


Время запуска задачи.

```
RandomInterval=<мин.>
```

Интервал запуска задачи, если несколько задач запущены одновременно (в минутах).

```
RunMissedStartRules
```

Включает или выключает запуск пропущенной задачи после запуска программы Kaspersky Endpoint Security.

Примеры:

Чтобы настроить запуск задачи каждые 10 часов, укажите следующие параметры:

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2019/May/30 23:05:00;10
RandomInterval=0
```

Чтобы настроить запуск задачи каждые 10 минут, укажите следующие параметры:

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

Чтобы настроить запуск задачи 15-го числа каждого месяца, укажите следующие параметры:

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

Чтобы настроить запуск задачи каждый вторник, укажите следующие параметры:

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

Чтобы настроить запуск задачи через каждые 11 дней, укажите следующие параметры:

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Использование логических выражений

Логические выражения можно использовать, чтобы ограничить результаты запроса для следующих команд:

- Получить информацию о событиях Kaspersky Endpoint Security:
`-E --query "<логическое выражение>"`
- Получить информацию о файлах в хранилище:
`-Q --query "<логическое выражение>"`
- Удалить выбранные объекты из хранилища:
`-Q --mass-remove --query "<логическое выражение>"`

Можно указать несколько фильтров, комбинируя их с помощью логического оператора AND. Закрывайте логические выражения в кавычки.

Синтаксис

"<поле> <логический оператор> '<значение>' "

"<поле> <логический оператор> '<значение>' и <поле> <логический оператор> '<значение>' "

Таблица 3. Описание логических операторов

Логический оператор	Описание
>	Больше
<	Меньше
like	Соответствует указанному значению (при указании значения можно использовать маски %, см. пример ниже)
==	Равно
!=	Не равно
>=	Больше или равно
<=	Меньше или равно

Примеры:

Вывести информацию о файлах в хранилище, имеющих Высокий (High) уровень важности:

```
-Q --query "DangerLevel == 'High'"
```

Вывести информацию о событиях, которые содержат текст “etc” в поле FileName:

```
-E --query "FileName like '%etc%'"
```

Вывести события с типом ThreatDetected (обнаружена угроза):

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Вывести события с типом ThreatDetected (обнаружена угроза), сформированные задачами ODS:

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Вывести события, сформированные после даты, указанной в системе отметок времени UNIX (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года):

```
kesl-control -E --query "Date > '1583425000'"
```

Экспорт и импорт параметров программы

Kaspersky Endpoint Security позволяет вам импортировать и экспортировать все параметры программы для диагностики сбоев, проверки параметров или для упрощения настройки программы на компьютерах.

При *экспорте* параметров все параметры программы и задач сохраняются в конфигурационном файле. Этот конфигурационный файл используется, чтобы *импортировать* параметры для настройки программы.

Во время импорта или экспорта параметров Kaspersky Endpoint Security должен быть запущен. После импорта параметров требуется перезапустить программу.

Если вы управляете программой через Kaspersky Security Center, импорт параметров недоступен.

Импорт параметров в предыдущую версию программы недоступен.

При импорте или экспорте параметров из предыдущей версии программы для новых параметров устанавливаются значения по умолчанию.

При импорте параметров программы в сертифицированной версии программы для параметра UseKSN устанавливается значение No. Чтобы начать или возобновить участие в Kaspersky Security Network, требуется ввести UseKSN=Basic или UseKSN=Extended (см. раздел “Участие в Kaspersky Security Network” на стр. [162](#)).

При импорте параметров в сертифицированной версии программы также устанавливается следующее значение для параметра задачи обновления: ApplicationUpdateMode=Disabled.

Параметры задач Управление сетевым экраном (Firewall), Контроль устройств (Device Control) и Защита от сетевых угроз (Network_Threat_Protection) не импортируются, так как эти задачи недоступны.

После импорта параметров программы внутренние идентификаторы задач могут поменяться. Для управления ими рекомендуется использовать имена задач.

- ▶ *Чтобы экспортировать параметры программы в конфигурационный файл, выполните следующую команду:*

```
kesl-control --export-settings [--file <полный путь к конфигурационному файлу>]
```

- ▶ *Чтобы настроить программу с помощью параметров из конфигурационного файла (импортировать параметры), выполните следующую команду:*

```
kesl-control --import-settings --file <полный путь к конфигурационному файлу>
```

Управление задачами Kaspersky Endpoint Security с помощью командной строки

Этот раздел содержит информацию о типах задач Kaspersky Endpoint Security и инструкции о том, как управлять задачами.

В этой главе

О задачах Kaspersky Endpoint Security	69
Просмотр списка задач Kaspersky Endpoint Security	71
Создание задачи	72
Изменение параметров задачи с помощью конфигурационного файла	73
Изменение параметров задачи с помощью командной строки	73
Восстановление заданных по умолчанию параметров задачи из командной строки	74
Запуск и остановка задачи	74
Управление областями проверки из командной строки	75
Управление исключенными областями из командной строки	75
Просмотр состояния задачи	76
Настройка расписания задачи	76
Получение параметров расписания задачи	77
Изменение параметров расписания задачи	77
Удаление задачи	78

О задачах Kaspersky Endpoint Security

Вы можете управлять работой Kaspersky Endpoint Security с помощью задач как локально на компьютере (с помощью командной строки или конфигурационных файлов), так и централизованно с помощью Kaspersky Security Center (см. раздел “Управление программой с помощью Kaspersky Security Center” на стр. [170](#)).

Для работы с Kaspersky Endpoint Security предусмотрено два типа задач:

- *Предустановленная задача* – задача, которая создается во время установки программы. Вы не можете создавать или удалять предустановленные задачи, но вы можете изменять параметры этих задач.
- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно.

Задачи Kaspersky Endpoint Security перечислены в следующей таблице.

Таблица 4. Задачи Kaspersky Endpoint Security

Название задачи	ID задачи	Тип задачи	Возможность создавать пользовательские задачи этого типа
File_Threat_Protection (см. раздел “Задача Защита от файловых угроз (File_Threat_Protection ID:1)” на стр. 79)	1	OAS	Нет
Scan_My_Computer (см. раздел “Задача антивирусной проверки (Scan_My_Computer ID:2)” на стр. 89)	2	ODS	Да
Scan_File (см. раздел “Задача выборочной проверки (Scan_File ID:3)” на стр. 97)	3	ODS	Да
Boot_Scan (см. раздел “Задача проверки загрузочных секторов (Boot_Scan ID:4)” на стр. 105)	4	BootScan	Да
Memory_Scan (см. раздел “Задача проверки памяти процессов и памяти ядра (Memory_Scan ID:5)” на стр. 108)	5	MemoryScan	Да
Update (см. раздел “Задача обновления (Update ID:6)” на стр. 110)	6	Update	Да
Rollback (см. раздел “Задача Откат обновления баз (Rollback ID:7)” на стр. 115)	7	Rollback	Да
License (см. раздел “Задача Лицензирование (License ID:9)” на стр. 116)	9	License	Нет
Backup (см. раздел “Задача Управление Хранилищем (Backup ID:10)” на стр. 118)	10	Backup	Нет
System_Integrity_Monitoring (см. раздел “Задача Контроль целостности системы (System_Integrity_Monitoring ID:11)” на стр. 122)	11	OAFIM	Нет
Firewall_Management (задача Управление сетевым экраном)	12	Firewall	Нет
Anti_Cryptor (см. раздел “Задача Защита от шифрования (AntiCryptor ID:13)” на стр. 130)	13	AntiCryptor	Нет
Web_Threat_Protection (см. раздел “Задача Защита от веб-угроз (Web_Threat_Protection ID: 14)” на стр. 136)	14	WTP	Нет
Device_Control (задача Контроль устройств)	15	DeviceControl	Нет
Removable_Drives_Scan (см. раздел “Задача Проверка съемных дисков (Removable_Drives_Scan ID: 16)” на стр. 139)	16	RDS	Нет
Network_Threat_Protection (задача Защита от сетевых угроз)	17	NTP	Нет
Container_Scan (см. раздел “Задача Проверка контейнеров (Container_Scan ID: 18)” на стр. 141)	18	ContainerScan	Да

Custom_Container_Scan (см. раздел “Задача Выборочная проверка контейнеров (Container_Scan ID: 19)” на стр. 150)	19	ContainerScan	Нет
Behavior_Detection (см. раздел “Задача Анализ поведения (Behavior_Detection ID: 20)” на стр. 158)	20	BehaviorDetection	Нет

ID – номер задачи, который программа Kaspersky Endpoint Security присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются с 100. Все задачи, включая удаленные, имеют уникальные идентификаторы. Программа не использует повторно идентификаторы удаленных задач. Идентификатор новой задачи представляет собой номер, следующий по порядку за идентификатором последней созданной задачи.

Названия задач не чувствительны к регистру.

В сертифицированной версии программы задачи Управление сетевым экраном, Контроль устройств и Защита от сетевых угроз недоступны.

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать задачи;
- создавать и удалять пользовательские задачи;
- изменять параметры задач.

Просмотр списка задач Kaspersky Endpoint Security

► Чтобы просмотреть список задач Kaspersky Endpoint Security, выполните следующую команду:

```
kesl-control [-T] --get-task-list
```

Отобразится список, в котором представлены задачи Kaspersky Endpoint Security.

Для каждой задачи отображается следующая информация:

- **Название.** Название задачи (см. раздел “О задачах Kaspersky Endpoint Security” на стр. [69](#)).
- **ID.** Идентификатор задачи (см. раздел “О задачах Kaspersky Endpoint Security” на стр. [69](#)).
- **Type.** Тип задачи (см. раздел “О задачах Kaspersky Endpoint Security” на стр. [69](#)).
- **State.** Текущее состояние задачи (см. раздел “Просмотр состояния задачи” на стр. [76](#)).

Если политика Kaspersky Security Center запрещает пользователям просматривать и изменять параметры задач локально, отображается информация только о задачах Scan_File, Backup, License, File_Threat_Protection, System_Integrity_Monitoring и Anti_Cryptor. Информация о других задачах недоступна.

Если ваша лицензия не предоставляет функции Защита от шифрования (см. раздел “Задача Защита от шифрования (AntiCryptor ID:13)” на стр. [130](#)) и Контроль целостности системы (см. раздел “Задача Контроль целостности системы (System_Integrity_Monitoring ID:11)” на стр. [122](#)), информация о соответствующих задачах не отображается.

Создание задачи

Вы можете создавать задачи с параметрами по умолчанию или параметрами, указанными в конфигурационном файле.

Вы можете создавать только задачи следующих типов: ODS, BootScan, MemoryScan, Update, Rollback и ContainerScan.

- ▶ Чтобы создать задачу с параметрами по умолчанию, выполните следующую команду:

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи>
```

где:

- <имя задачи> – имя, которое вы указываете для новой задачи;
- <тип задачи> – стандартный тип задачи (см. раздел “О задачах Kaspersky Endpoint Security” на стр. [69](#)).

Задача указанного типа создается с параметрами по умолчанию.

- ▶ Чтобы создать задачу с параметрами, указанным в конфигурационном файле, выполните следующую команду:

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи> --file  
<полный путь к конфигурационному файлу>
```

где:

- <имя задачи> – имя, которое вы указываете для новой задачи;
- <тип задачи> – предустановленный тип задачи (см. раздел “О задачах Kaspersky Endpoint Security” на стр. [69](#)).
- <полный путь к конфигурационному файлу> – полный путь к конфигурационному файлу (см. раздел “Конфигурационные файлы задачи по умолчанию” на стр. [198](#)).

Задача указанного типа создается с параметрами, указанными в конфигурационном файле.

Изменение параметров задачи с помощью конфигурационного файла

► Чтобы изменить параметры задачи путем изменения конфигурационного файла, выполните следующие действия:

1. Сохраните параметры задачи в конфигурационный файл:

```
kesl-control --get-settings <имя задачи>|<task ID> --file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Измените нужный параметр в конфигурационном файле.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте в задачу параметры из конфигурационного файла:

```
kesl-control --set-settings <имя задачи>|<task ID> --file <полный путь к файлу>
```

В результате параметры задачи будут обновлены.

Изменение параметров задачи с помощью командной строки

► Чтобы изменить параметры задачи с помощью командной строки, выполните следующие действия:

1. Укажите нужное значение параметра:

```
kesl-control --set-settings <имя или идентификатор задачи>  
setting=value [параметр=значение]
```

Программа Kaspersky Endpoint Security изменит указанный параметр.

2. Убедитесь, что значение параметра изменено в конфигурационном файле задачи:

```
kesl-control --get-settings <имя или идентификатор задачи>
```

Если вы добавили новую область проверки или область исключения без указания всех параметров, область будет добавлена в конфигурационный файл с параметрами по умолчанию.

Пример:

Чтобы указать новую область проверки, выполните следующую команду:

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes  
ScanScope.item_0001.Path=/home
```

В конфигурационный файл будет добавлен новый раздел с описанием области проверки для задачи с ID=100:

```
[ScanScope.item_0001]  
  
AreaDesc=  
  
UseScanArea=Yes  
  
Path=/home  
  
AreaMask.item_0000=*
```

Восстановление заданных по умолчанию параметров задачи из командной строки

Kaspersky Endpoint Security позволяет восстановить заданные по умолчанию параметры задачи из командной строки.

Восстановление заданных по умолчанию параметров не доступно для задач Откат обновлений (см. раздел “Задача Откат обновлений (Rollback ID:7)” на стр. [115](#)) и Управление хранилищем (см. раздел “Задача Управление хранилищем (Backup ID:10)” на стр. [118](#)).

► Чтобы восстановить заданные по умолчанию параметры задачи из командной строки, выполните следующие действия:

1. Выполните следующую команду:

```
kesl-control --set-settings <ID задачи>|<имя задачи> --set-to-default
```

Программа Kaspersky Endpoint Security изменит значения параметров на заданные по умолчанию.

2. Убедитесь, что значения параметров изменены в конфигурационном файле задачи:

```
kesl-control --get-settings <ID задачи>|<имя задачи> --file <имя  
конфигурационного файла>
```

В конфигурационном файле задачи содержатся заданные по умолчанию значения всех параметров.

Запуск и остановка задачи

Вы не можете запускать и останавливать задачи типов Backup и License.

- ▶ Чтобы запустить задачу, выполните следующую команду:

```
kesl-control --start-task <ID задачи>|<имя задачи>
```

- ▶ Чтобы остановить задачу, выполните следующую команду:

```
kesl-control --stop-task <ID задачи>|<имя задачи>
```

Управление областями проверки из командной строки

Вы можете добавлять или удалять область проверки с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и AntiCryptor из командной строки.

- ▶ Чтобы добавить новую область проверки, выполните следующую команду:

```
kesl-control --set-settings <ID или название задачи> --add-path <путь>
```

В конфигурационный файл будет добавлен новый раздел `[ScanScope.item_#]`. Kaspersky Endpoint Security будет проверять объекты в директории, указанной в параметре `Path`.

Если для указанного параметра `Path` уже существует раздел `[ScanScope.item_#]`, дублирующийся раздел не добавляется в конфигурационный файл. Если для параметра `UseScanArea` указано значение `No`, после выполнения этой команды значение изменяется на `Yes` и будет выполняться проверка объектов, расположенных в этой директории.

- ▶ Чтобы удалить область проверки, выполните следующую команду:

```
kesl-control --set-settings <ID или название задачи> --del-path <путь>
```

Раздел `[ScanScope.item_#]`, содержащий указанный путь, удаляется из конфигурационного файла задачи. Kaspersky Endpoint Security не будет проверять объекты в директории, указанной в параметре `Path`.

Управление исключенными областями из командной строки

Вы можете добавлять или удалять область исключения с указанным параметром `Path` для задач OAS, ODS, OAFIM, ODFIM и AntiCryptor из командной строки.

- ▶ Чтобы добавить новую область исключения, выполните следующую команду:

```
kesl-control --set-settings <ID или название задачи> --add-exclusion  
<путь>
```

В конфигурационный файл будет добавлен новый раздел `[ExcludedFromScanScope.item_#]`. Kaspersky Endpoint Security будет исключать объекты, расположенные в директории, указанной в параметре `Path`. Если для указанного параметра `Path` уже существует раздел `[ExcludedFromScanScope.item_#]`, дублирующийся раздел не добавляется в конфигурационный файл. Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменяется на `Yes` и объекты, расположенные в этой директории, исключаются из проверки.

- ▶ Чтобы удалить область исключения, выполните следующую команду:

```
kesl-control --set-settings <ID или название задачи> --del-exclusion  
<путь>
```

Раздел [ExcludedFromScanScope.item_#], содержащий указанный путь, будет удален из конфигурационного файла задачи. Kaspersky Endpoint Security не будет исключать объекты, расположенные в директории, указанной в параметре Path.

Просмотр состояния задачи

Вы можете просматривать состояние задачи.

- ▶ Чтобы просмотреть состояние задачи, выполните следующую команду:

```
kesl-control --get-task-state <ID задачи>|<имя задачи>
```

где:

- <ID задачи> – идентификатор задачи, который программа Kaspersky Endpoint Security присвоила задаче в момент создания.
- <название задачи> – название задачи.

Задачи Kaspersky Endpoint Security могут находиться в одном из следующих состояний:

- Started – задача запущена.
- Starting – задача запускается.
- Stopped – задача остановлена.
- Stopping – задача останавливается.

Настройка расписания задачи

- ▶ Чтобы настроить расписание задачи, выполните следующие действия:

1. Сохраните параметры расписания задачи в конфигурационный файл с помощью следующей команды:

```
kesl-control --get-schedule <ID задачи>|<имя задачи>
```

2. Откройте конфигурационный файл для редактирования.
3. Задайте параметры расписания.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры расписания в задачу с помощью следующей команды:

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <полный  
путь к файлу>
```

Получение параметров расписания задачи

Команда `kesl-control --get-schedule` выводит параметры расписания задачи. Используя эту команду, вы также можете получить параметры расписания задачи, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения расписания задачи:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `kesl-control --get-schedule`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `kesl-control --set-schedule`.

Kaspersky Endpoint Security применит новые значения параметров расписания.

Синтаксис команды

```
kesl-control [-T] --get-schedule <ID задачи>|<имя задачи> [--file <имя конфигурационного файла>]
```

```
kesl-control [-T] --get-schedule <ID задачи>|<имя задачи> <название параметра>
```

Аргументы и ключи

<ID задачи>

Идентификационный номер задачи в Kaspersky Endpoint Security.

<имя задачи>

Имя задачи.

--file <имя конфигурационного файла>

Имя конфигурационного файла, в котором будут сохранены параметры расписания. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Пример:

Сохранить параметры Kaspersky Endpoint Security в файле с именем `update_schedule.ini`. Сохранить созданный файл в текущей директории:

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

Изменение параметров расписания задачи

Команда `kesl-control --set-schedule` задает параметры расписания задачи с помощью ключей команды или импортирует параметры расписания задачи из указанного конфигурационного файла.

Вы можете использовать эту команду для изменения параметров Kaspersky Endpoint Security:

1. Сохраните параметры расписания в конфигурационном файле, выполнив команду `kesl-control --get-schedule`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security, выполнив команду `kesl-control --set-schedule`.

Kaspersky Endpoint Security применит новые значения параметров расписания.

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <имя конфигурационного файла>
```

```
kesl-control --set-schedule <ID задачи>|<имя задачи> <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

Аргументы и ключи

<ID задачи>

Идентификационный номер задачи в Kaspersky Endpoint Security.

<имя задачи>

Имя задачи.

--file <имя конфигурационного файла>

Имя конфигурационного файла, параметры расписания из которого будут импортированы в задачу; включает полный путь к файлу.

Пример:

Импортировать в задачу с ID=2 параметры расписания из конфигурационного файла с именем `/home/test/on_demand_schedule.ini`:

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Удаление задачи

Вы можете удалять задачи, которые вы создали.

- Чтобы удалить задачу, выполните следующую команду:

```
kesl-control --delete-task <ID задачи>|<имя задачи>
```

Задача Защита от файловых угроз (File_Threat_Protection ID:1)

В этом разделе содержится информация о задаче Защита от файловых угроз.

В этой главе

О защите от файловых угроз.....	79
Особенности проверки символических и жестких ссылок	80
Параметры задачи Защита от файловых угроз	80
Формирование глобальной области исключения	87

О защите от файловых угроз

Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. Задача Защита от файловых угроз создается автоматически с параметрами по умолчанию при установке Kaspersky Endpoint Security на компьютер. По умолчанию задача Защита от файловых угроз запускается автоматически при старте Kaspersky Endpoint Security. Задача постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Во время работы задачи Защита от файловых угроз Kaspersky Endpoint Security выполняет проверку всех пространств имен во всех поддерживаемых операционных системах, если в общих параметрах программы для параметра `NamespaceMonitoring` задано значение `Yes` (см. раздел “Общие параметры Kaspersky Endpoint Security” на стр. [52](#)).

Дополнительно для операционной системы Astra Linux пользовательская задача антивирусной проверки (Scan_File) позволяет проверять файлы из других пространств имен (в рамках обязательной проверки).

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуются права роли Администратор.

Вы не можете создавать пользовательские задачи Защита от файловых угроз. Вы можете изменить параметры задачи Защиты от файловых угроз, созданной по умолчанию (см. раздел “Управление задачами Kaspersky Endpoint Security с помощью командной строки” на стр. [69](#)).

Параметры постоянной защиты содержатся в конфигурационном файле, который используется в задаче Защита от файловых угроз.

О зараженных файлах

При проверке файлов Kaspersky Endpoint Security использует антивирусные базы. Базы содержат файлы с фрагментами кода угроз и алгоритмы лечения объектов, в которых содержатся эти угрозы. Антивирусные базы позволяют обнаруживать в проверяемых файлах известные угрозы.

Если в файле содержится код, который полностью совпадает с кодом известной угрозы, Kaspersky Endpoint Security присваивает файлу статус Зараженный.

Особенности проверки символических и жестких ССЫЛОК

Программа Kaspersky Endpoint Security позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Программа Kaspersky Endpoint Security проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область защиты задачи Защита от файловых угроз.

Если файл, обращение к которому происходит по символической ссылке, не входит в область задачи Защита от файловых угроз, программа не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность компьютера окажется под угрозой.

Проверка жестких ссылок

При обработке файла, у которого больше одной жесткой ссылки, программа Kaspersky Endpoint Security выбирает действие в зависимости от заданного действия над объектами:

- Если выбрано действие **Выполнять рекомендуемое действие** (Recommended), Kaspersky Endpoint Security автоматически подбирает и выполняет действие над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности его лечения.
- Если выбрано действие **Удалять** (Remove), Kaspersky Endpoint Security удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.
- Если выбрано действие **Лечить** (Disinfect), Kaspersky Endpoint Security лечит исходный файл. Если лечение невозможно, программа удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки.

Когда вы восстанавливаете файл с жесткой ссылкой из Хранилища, Kaspersky Endpoint Security создает копию исходного файла с именем жесткой ссылки, которая была помещена в хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Параметры задачи Защита от файловых угроз

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от файловых угроз.

Ниже приведены все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.

Доступные значения:

Yes – проверять архивы. Если указано значение `FirstAction=Recommended`, то в зависимости от типа архива программа удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу.

No – не проверять архивы.

Значение по умолчанию: No

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

Yes – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: No.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook®, Outlook Express, The Bat! и других.

Доступные значения:

Yes – проверять файлы почтовых баз;

No – не проверять файлы почтовых баз.

Значение по умолчанию: No.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: No.

SizeLimit

Задаёт максимальный размер проверяемого архива (в мегабайтах). Если размер проверяемого архива превышает указанное значение, Kaspersky Endpoint Security пропускает этот архив.

Доступные значения:

0 – 999,999

0 – Kaspersky Endpoint Security проверяет архивы любого размера.

Значение по умолчанию: 0.

TimeLimit

Задаёт максимальную продолжительность проверки архива (в секундах). Kaspersky Endpoint Security прекращает проверку архива, если она выполняется дольше, чем указано значением этого параметра.

Доступные значения:

0 – 9999

0 – продолжительность проверки архивов не ограничена.

Значение по умолчанию: 60.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над зараженными объектами.

В задаче Защита от файловых угроз, перед тем как выполнить над объектом выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к этому объекту для программ, которые к нему обращаются.

Доступные значения:

Disinfect (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано **Disinfect**, рекомендуется задать второе действие в параметре **SecondAction**.

Remove (удалять) – Kaspersky Endpoint Security удаляет зараженный объект, предварительно создав его резервную копию.

Recommended (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

Block (блокировать) – Kaspersky Endpoint Security блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: **Recommended**.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над зараженными объектами. Kaspersky Endpoint Security выполняет второе действие, если не удалось выполнить первое действие.

Значения параметра **SecondAction** такие же, как значения параметра **FirstAction**.

Если в качестве первого действия выбрано **Block** (блокировать) или **Remove** (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, Kaspersky Endpoint Security в качестве второго действия применяет **Block** (блокировать).

Значение по умолчанию: **Block**.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром **ExcludeMasks**.

Доступные значения:

Yes – исключать объекты, указанные параметром **ExcludeMasks**.

No – не исключать объекты, указанные параметром **ExcludeMasks**.

Значение по умолчанию: **No**.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=Yes  
ExcludeMasks.item_0000=eicar1.*  
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа Kaspersky Endpoint Security не блокировала ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<https://encyclopedia.kaspersky.ru/>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes  
ExcludeThreats.item_0000=EICAR-Test-*  
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые программа Kaspersky Endpoint Security признала незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о незараженных объектах;

No – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: No.

ReportPackedObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о проверке объектов в составе архивов;

No – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: No.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

Yes – записывать в журнал информацию о непроверенных объектах;

No – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: No.

UseAnalyzer

Включает или отключает эвристический анализатор.

Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и

длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

`Light` – наименее тщательная проверка, минимальная загрузка системы;

`Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы;

`Deep` – наиболее тщательная проверка, максимальная загрузка системы;

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

С помощью этого параметра можно указать режим задачи Защита от файловых угроз. Параметр `ScanByAccessType` применяется только в задаче Защита от файловых угроз.

Доступные значения:

`SmartCheck` – проверять файл при попытке открытия, и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом.

`OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.

`Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.

Значение по умолчанию: `SmartCheck`.

В разделе `[ScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: `All objects`.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Этот параметр включает или отключает проверку указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.

Доступные значения:

Yes – проверять указанную область;

No – не проверять указанную область.

Значение по умолчанию: Yes.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: * (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра Path включает два элемента: <тип файловой системы>:<протокол доступа>. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

<путь к локальной директории> – проверять объекты в указанной директории;

Shared:NFS – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

Shared:SMB – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB;

AllRemoteMounted – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

AllShared – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

В разделе [ExcludedFromScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

Yes – исключать указанную область;

No – не исключать указанную область.

Значение по умолчанию: Yes.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра Path включает два элемента: <тип файловой системы>:<протокол доступа>. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

<путь к локальной директории> – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir*/file или /dir*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/***/file – это неправильная маска.

Shared:NFS – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS;

Shared:SMB – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba;

AllRemoteMounted – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

AllShared – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

Формирование глобальной области исключения

Вы можете указать глобальную область исключения для задачи Защита от файловых угроз. Файлы в глобальной области исключения исключаются из области постоянной защиты.

► Чтобы создать глобальную область исключения, выполните следующие действия:

1. Сохраните параметры задачи Защита от файловых угроз в файл с помощью следующей команды:

```
kesl-control --get-settings 1 --file <полный путь к конфигурационному файлу>
```

2. Добавьте в созданный файл блок [ExcludedFromScanScope.item_#]. В каждом блоке [ExcludedFromScanScope.item_#] содержатся следующие параметры:

- AreaMask – маски имени файла для файлов, которые требуется исключить из области защиты.
- AreaDesc – описание области исключений, содержащее дополнительную информацию об области исключения.
- Path – путь к файлам или директориям, которые требуется исключить из области защиты.

Пример:

```
[ExcludedFromScanScope.item_0000]  
AreaDesc=  
UseScanArea=Yes  
Path=/tmp/notchecked  
AreaMask.item_0000=*
```

3. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

```
kesl-control --set-settings 1 --file <полный путь к конфигурационному файлу>
```

Управлять исключенными областями можно также из командной строки (см. раздел “Управление исключенными областями из командной строки” на стр. [75](#)).

Задача антивирусной проверки (Scan_My_Computer ID:2)

В этом разделе содержится информация о задаче антивирусной проверки.

В этой главе

Об антивирусной проверке	89
Параметры задачи антивирусной проверки	89

Об антивирусной проверке

Антивирусная проверка – это однократная полная или выборочная проверка файлов на компьютере, выполняемая программой Kaspersky Endpoint Security. Kaspersky Endpoint Security может выполнять несколько задач антивирусной проверки одновременно.

По умолчанию в программе Kaspersky Endpoint Security создается одна предустановленная задача антивирусной проверки – *полная проверка*. Программа проверяет все объекты, расположенные на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Пользователи могут создавать пользовательские задачи антивирусной проверки. По умолчанию в программе Kaspersky Endpoint Security также создается предустановленная пользовательская задача антивирусной проверки.

Если программа была перезапущена контрольной службой или вручную пользователем во время антивирусной проверки, выполнение задачи прерывается. В журнале программы сохраняется событие *OnDemandTaskInterrupted*.

Параметры задачи антивирусной проверки

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи антивирусной проверки.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj.

Доступные значения:

Yes – проверять архивы; Если указано значение *FirstAction=Recommended*, программа удаляет архив, содержащий угрозу.

No – не проверять архивы.

Значение по умолчанию: Yes.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

`No` – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: `Yes`.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.

Доступные значения:

`Yes` – проверять файлы почтовых баз;

`No` – не проверять файлы почтовых баз.

Значение по умолчанию: `No`.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

`Yes` – проверять сообщения электронной почты в текстовом формате;

`No` – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: `No`.

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

`Idle` – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Idle`.

SizeLimit

Задаёт максимальный размер проверяемого архива (в мегабайтах). Если размер проверяемого архива превышает указанное значение, Kaspersky Endpoint Security пропускает этот архив.

Доступные значения:

`0` – 999,999

0 – Kaspersky Endpoint Security проверяет архивы любого размера.

Значение по умолчанию: 0.

TimeLimit

Задаёт максимальную продолжительность проверки архива (в секундах). Kaspersky Endpoint Security прекращает проверку архива, если она выполняется дольше, чем указано значением этого параметра.

Доступные значения:

0 – 9999

0 – продолжительность проверки архивов не ограничена.

Значение по умолчанию: 0.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над заражёнными объектами.

Если заражённый объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие *Удалить*, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

Disinfect (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), программа Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано *Disinfect*, рекомендуется задать второе действие в параметре *SecondAction*.

Remove (удалять) – Kaspersky Endpoint Security удаляет заражённый объект, предварительно создав его резервную копию.

Recommended (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

Skip (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить заражённый объект. Информация о заражённом объекте сохраняется в журнале.

Значение по умолчанию: *Recommended*.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над заражёнными объектами. Kaspersky Endpoint Security выполняет второе действие, если не удалось выполнить первое действие.

Значения параметра *SecondAction* такие же, как значения параметра *FirstAction*.

Если в качестве первого действия выбрано *Skip* (пропускать) или *Remove* (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, Kaspersky Endpoint Security в качестве второго действия применяет *Skip* (пропускать).

Значение по умолчанию: `Skip`.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=yes
ExcludeMasks.item_0000=eicar1.*
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа Kaspersky Endpoint Security не блокировала ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<https://encyclopedia.kaspersky.ru/>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes
```

```
ExcludeThreats.item_0000=EICAR-Test-*
```

```
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые программа Kaspersky Endpoint Security признала незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о незараженных объектах;

No – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: **No**.

ReportPackedObjects

Включает или отключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о проверке объектов в составе архивов;

No – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: **No**.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

Yes – записывать в журнал информацию о непроверенных объектах;

No – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: **No**.

UseAnalyzer

Включает или отключает эвристический анализатор.

Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

Light – наименее тщательная проверка, минимальная загрузка системы;

Medium – средний уровень эвристического анализа, сбалансированная загрузка системы;

Deep – наиболее тщательная проверка, максимальная загрузка системы;

Recommended – рекомендуемое значение.

Значение по умолчанию: Recommended.

UseIChecker

Включает или отключает использование технологии iChecker.

Доступные значения:

Yes – включить использование технологии iChecker;

No – отключить использование технологии iChecker.

Значение по умолчанию: Yes.

В разделе [ScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: All objects.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Включает или выключает проверку указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.

Доступные значения:

Yes – проверять указанную область;

No – не проверять указанную область.

Значение по умолчанию: Yes.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: * (проверять все объекты).

Пример:

```
AreaMask_<номер элемента>=* .doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра Path включает два элемента: <тип файловой системы>:<протокол доступа>. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

<путь к локальной директории> – проверять объекты в указанной директории;

Shared:NFS – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS;

Shared:SMB – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу SMB;

AllRemoteMounted – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

AllShared – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

В разделе [ExcludedFromScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски для имени файла или директории. Один символ `*` можно указать вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/file`.

Два последовательно идущих символа `*` можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir**/file/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

Задача выборочной проверки (Scan_File ID:3)

В этом разделе содержится информация о задаче выборочной проверки.

В этой главе

О задаче выборочной проверки	97
Параметры задачи выборочной проверки.....	97

О задаче выборочной проверки

Задача выборочной проверки использует параметры, которые применяются командой `kesl-control --scan-file`.

Вы можете проверить файл или директорию с помощью следующей команды:

```
kesl-control --scan-file <путь к файлу>
```

Программа создает временную задачу антивирусной проверки (тип=ODS) с параметрами задачи Scan_File. После завершения проверки временная задача автоматически удаляется.

Вы можете изменить параметры проверки для временной задачи Scan_File из командной строки.

Параметры задачи выборочной проверки

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи выборочной проверки.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanArchived

Включение или отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их. Поддерживаются следующие типы архивов: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.

Доступные значения:

Yes – проверять архивы; Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

No – не проверять архивы.

Значение по умолчанию: Yes.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

Yes – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: *Yes*.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.

Доступные значения:

Yes – проверять файлы почтовых баз;

No – не проверять файлы почтовых баз.

Значение по умолчанию: *No*.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: *No*.

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

Idle – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

Normal – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: *Normal*.

SizeLimit

Задаёт максимальный размер проверяемого архива (в мегабайтах). Если размер проверяемого архива превышает указанное значение, Kaspersky Endpoint Security пропускает этот архив.

Доступные значения:

0 – 999, 999

0 – Kaspersky Endpoint Security проверяет архивы любого размера.

Значение по умолчанию: 0.

TimeLimit

Задаёт максимальную продолжительность проверки архива (в секундах). Kaspersky Endpoint Security прекращает проверку архива, если она выполняется дольше, чем указано значением этого параметра.

Доступные значения:

0 – 9999

0 – продолжительность проверки архивов не ограничена.

Значение по умолчанию: 0.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над заражёнными объектами.

Если заражённый объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие **Удалить**, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

Disinfect (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано **Disinfect**, рекомендуется задать второе действие в параметре **SecondAction**.

Remove (удалять) – Kaspersky Endpoint Security удаляет заражённый объект, предварительно создав его резервную копию.

Recommended (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

Skip (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить заражённый объект. Информация о заражённом объекте сохраняется в журнале.

Значение по умолчанию: **Recommended**.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над заражёнными объектами. Kaspersky Endpoint Security выполняет второе действие, если не удалось выполнить первое действие.

Значения параметра **SecondAction** такие же, как значения параметра **FirstAction**.

Если в качестве первого действия выбрано **Skip** (пропускать) или **Remove** (удалять), то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, Kaspersky Endpoint Security в качестве второго действия применяет **Skip** (пропускать).

Значение по умолчанию: **Skip**.

UseExcludeMasks

Включает или отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию не задано.

Пример:

```
UseExcludeMasks=Yes
ExcludeMasks.item_0000=eicar1.*
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа Kaspersky Endpoint Security не блокировала ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<https://encyclopedia.kaspersky.ru/>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

Пример:

```
UseExcludeThreats=Yes
```

```
ExcludeThreats.item_0000=EICAR-Test-*
```

```
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые программа Kaspersky Endpoint Security признала незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о незараженных объектах;

No – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: No.

ReportPackedObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен программой Kaspersky Endpoint Security.

Доступные значения:

Yes – записывать в журнал информацию о проверке объектов в составе архивов;

No – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: No.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о непроверенных объектах.

Доступные значения:

Yes – записывать в журнал информацию о непроверенных объектах;

No – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: No.

UseAnalyzer

Включает или выключает эвристический анализатор.

Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

Light – наименее тщательная проверка, минимальная загрузка системы;

Medium – средний уровень эвристического анализа, сбалансированная загрузка системы;

Deep – наиболее тщательная проверка, максимальная загрузка системы;

Recommended – рекомендуемое значение.

Значение по умолчанию: Recommended.

UseChecker

Включает или выключает использование технологии iChecker.

Доступные значения:

Yes – включить использование технологии iChecker;

No – отключить использование технологии iChecker.

Значение по умолчанию: Yes.

В разделе [ScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.

Значение по умолчанию: All objects.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Включает или выключает проверку указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.

Доступные значения:

Yes – проверять указанную область;

No – не проверять указанную область.

Значение по умолчанию: `Yes`.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: `*` (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – проверять объекты в указанной директории;

`Shared:NFS` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS;

`Shared:SMB` – проверять ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу SMB;

`AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – проверять все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

В разделе `[ExcludedFromScanScope.item_#]` содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Включает или выключает проверку указанной области.

Доступные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` включает два элемента: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Доступные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски.

Можно использовать символ `*` (звездочка) для формирования маски для имени файла или директории. Один символ `*` можно указать вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/**/file`.

Два последовательно идущих символа `*` можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `.`. Например, `/dir/**/file/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, доступ к которым предоставляется по протоколам SMB и NFS.

Задача проверки загрузочных секторов (Boot_Scan ID:4)

Задача проверки загрузочных секторов позволяет проверять загрузочные сектора без указания области проверки.

Ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи проверки загрузочных секторов. Вы можете изменить значения параметра во время выполнения задачи из командной строки (см. раздел “Изменение параметров задачи с помощью командной строки” на стр. [73](#)).

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Disinfect` – Kaspersky Endpoint Security пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Disinfect`

UseExcludeMasks

Включает или отключает исключение объектов, указанных параметром `ExcludeMasks`, из проверки.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks.item_#

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.

Значение по умолчанию не задано.

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: No.

ExcludeThreats.item_#

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа Kaspersky Endpoint Security не блокировала ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<https://encyclopedia.kaspersky.ru/>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые программа Kaspersky Endpoint Security признала незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: No.

ReportUnprocessedObjects

Включает или выключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение `Yes` для этого параметра, так как запись большого объема информации может снизить производительность программы.

`No` – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: No

UseAnalyzer

Включает или выключает эвристический анализатор.

Эвристический анализ позволяет программе распознавать угрозы еще до того, как они станут известны вирусным аналитикам.

Доступные значения:

`Yes` – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Уровень эвристического анализа.

Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Доступные значения:

Light – наименее тщательная проверка, минимальная загрузка системы;

Medium – средний уровень эвристического анализа, сбалансированная загрузка системы;

Deep – наиболее тщательная проверка, максимальная загрузка системы;

Recommended – рекомендуемое значение.

Значение по умолчанию: Recommended.

DeviceNameMasks.item_#

Список масок имен проверяемых устройств. Требуется указать хотя бы одну маску имени устройства. Значение этого параметра не должно быть пустым.

Доступные значения:

AllObjects – проверять все устройства.

<маска имени устройства> – проверять устройства, имена которых содержат указанную маску.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir*/file или /dir*/*/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

Значение по умолчанию: /**/ – любой набор символов в имени маски устройства, включая символ /).

Задача проверки памяти процессов и памяти ядра (Memory_Scan ID:5)

Задача проверки памяти процессов и памяти ядра позволяет проверять память процессов и память ядра без указания области проверки.

Ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи проверки памяти процессов и памяти ядра.

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы программа Kaspersky Endpoint Security не блокировала ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<https://encyclopedia.kaspersky.ru/>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию не задано.

ReportCleanObjects

Включает или выключает запись в журнал информации о проверенных объектах, которые программа Kaspersky Endpoint Security признала незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен программой Kaspersky Endpoint Security.

Доступные значения:

`Yes` – записывать в журнал информацию о незараженных объектах;

`No` – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: `No`.

ReportUnprocessedObjects

Включает или выключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

`Yes` – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение `Yes` для этого параметра, так как запись большого объема информации может снизить производительность программы.

`No` – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: `No`

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Доступные значения:

`Disinfect` – Kaspersky Endpoint Security пытается вылечить объект. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: `Disinfect`

Задача обновления (Update ID:6)

В этом разделе содержится информация о задаче обновления.

В этой главе

Об обновлении баз и модулей программы.....	110
Об источниках обновлений	111
Параметры задач обновления.....	111
Установка обновления программы вручную	113

Об обновлении баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Для регулярного обновления требуется действительная лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений “Лаборатории Касперского”.

Для успешной загрузки пакета обновлений с серверов обновлений “Лаборатории Касперского” компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

В процессе обновления на ваш компьютер загружаются и устанавливаются базы программы Kaspersky Endpoint Security. Во время установки программа получает актуальные базы с одного из HTTP-серверов обновлений “Лаборатории Касперского”. Если для обновления используется предустановленная задача с параметрами по умолчанию (ID=6), Kaspersky Endpoint Security обновляет базы с периодичностью один раз в 60 минут. Вы можете изменять параметры предустановленной задачи обновления и создавать пользовательские задачи обновления.

Kaspersky Endpoint Security продолжает использовать предыдущую установленную версию баз, если загрузка обновлений баз прерывается или завершается с ошибкой. Если отсутствуют установленные ранее доступные базы программы, программа продолжает работу в режиме “без баз”. Обновление баз и модулей программы остается доступным.

Допускается устанавливать только обновления модулей программы, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу программы из сертифицированного состояния.

По умолчанию программа записывает в журнал событие *Базы устарели (AVBasesAreOutOfDate)*, если последние установленные обновления баз были опубликованы на сервере “Лаборатории Касперского” более трех дней назад. Если базы не обновлялись в течение семи дней, программа записывает в журнал

событие *Базы сильно устарели* (AVBasesAreTotallyOutOfDate). Базы актуальны, если они были загружены менее трех дней назад.

В процессе обновления программа и базы на вашем компьютере сравниваются с их актуальной версией, расположенной в *источнике обновлений*. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Об источниках обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security. Источником обновлений могут быть FTP- или HTTP-серверы (например, Kaspersky Security Center, серверы обновлений “Лаборатории Касперского”) и локальные или сетевые директории, смонтированные пользователем.

В предустановленной задаче обновления в качестве источника обновлений по умолчанию выбраны серверы обновлений “Лаборатории Касперского”. На серверах обновлений выкладываются обновления баз и программных модулей для многих программ “Лаборатории Касперского”. Обновления загружаются по протоколу HTTPS.

Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений “Лаборатории Касперского”, вы можете получать обновления из *пользовательского источника обновлений* – из указанной локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP- или HTTP-сервера. Вы можете указать пользовательский источник обновлений в конфигурационном файле задачи обновления.

Параметры задачи обновления

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи обновления.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

SourceType

С помощью этого параметра вы можете выбрать источник, из которого Kaspersky Endpoint Security будет получать обновления.

Доступные значения:

`KLServers` – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений “Лаборатории Касперского”. Обновления загружаются по протоколу HTTPS.

`SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.

`Custom` – Kaspersky Endpoint Security загружает обновления из пользовательского источника, указанного в разделе `[CustomSources.item_#]`. Вы можете указывать директории HTTP-

серверов или директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Значение по умолчанию: `KLServers`.

UseKLServersWhenUnavailable

С помощью этого параметра вы можете настроить обращение программы Kaspersky Endpoint Security к серверам обновлений “Лаборатории Касперского” в случае, если все пользовательские источники недоступны.

Доступные значения:

`Yes` – Kaspersky Endpoint Security подключается к серверам обновлений “Лаборатории Касперского”, если все пользовательские источники обновлений недоступны.

`No` – Kaspersky Endpoint Security не подключается к серверам обновлений “Лаборатории Касперского”, если все пользовательские источники обновлений недоступны.

Значение по умолчанию: `Yes`.

IgnoreProxySettingsForKLServers

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с серверами обновлений “Лаборатории Касперского”.

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для подключения к серверам обновлений “Лаборатории Касперского”.

`No` – Kaspersky Endpoint Security использует прокси-сервер для подключения к серверам обновлений “Лаборатории Касперского”.

Значение по умолчанию: `No`.

IgnoreProxySettingsForCustomSources

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с пользовательскими источниками обновлений. Вам нужно включить этот параметр, если для соединения с каким-либо из пользовательских HTTP-серверов обновлений требуется доступ к прокси-серверу.

Доступные значения:

`Yes` – Kaspersky Endpoint Security не использует прокси-сервер для подключения к пользовательским источникам обновлений.

`No` – Kaspersky Endpoint Security использует прокси-сервер для подключения к пользовательским источникам обновлений.

Значение по умолчанию: `No`.

ApplicationUpdateMode

Отображает режим загрузки и установки обновлений программы.

Доступные значения:

`Disabled` – не загружать и не устанавливать обновления программы.

`DownloadOnly` – загружать обновления программы, но не устанавливать их.

`DownloadAndInstall` – автоматически загружать и устанавливать обновления программы.

Значение по умолчанию: Disabled.

Для сохранения сертифицированной конфигурации программы значение параметра `ApplicationUpdateMode` должно быть Disabled.

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера при соединении с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, Kaspersky Endpoint Security обращается к другому указанному источнику обновлений.

Вы можете указывать только целые числа в диапазоне от 0 до 120.

Значение по умолчанию: 10.

Раздел `[CustomSources.item_#]` содержит следующие параметры:

URL

С помощью этого параметра вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Значение по умолчанию не задано.

Пример:

`URL=http://example.com/bases/` – адрес HTTP-сервера, на котором находится директория с обновлениями.

`URL=/home/bases/` – директория на защищаемом компьютере, в которой содержатся базы программы.

Enabled

С помощью этого параметра вы можете включить или отключить использование источника обновлений, указанного в параметре URL. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Доступные значения:

`Yes` – Kaspersky Endpoint Security использует источник обновлений.

`No` – Kaspersky Endpoint Security не использует источник обновлений.

Значение по умолчанию не задано.

Установка обновления программы вручную

Вы можете вручную установить обновление программы из командной строки. Для установки обновления на вашем компьютере должна быть установлена программа Kaspersky Endpoint Security. Для обновления программы Kaspersky Endpoint Security требуется остановить ее работу. Если процесс обновления

завершается с ошибкой, Kaspersky Endpoint Security автоматически откатывает обновления до предыдущей версии.

Пользователи сертифицированных версий могут устанавливать только обновления программы, прошедшие процедуру сертификации. Дистрибутивы обновленных версий доступны на веб-сайте <https://certifiedbuilds.kaspersky.ru/>.

Установка обновлений, не прошедших процедуру сертификации, приводит к выходу программы из сертифицированного состояния.

Задача Откат обновления баз (Rollback ID:7)

После первого обновления баз программы становится доступна функция отката баз программы к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, программа Kaspersky Endpoint Security создает резервную копию текущих баз программы. Это позволяет при необходимости откатить базы до предыдущей версии. Откат последних обновлений баз используется, например, если новая версия баз программы содержит недопустимые сигнатуры, что приводит к блокировке безопасных программ со стороны программы Kaspersky Endpoint Security.

Задача Откат обновления баз не имеет параметров.

Задача Лицензирование (License ID:9)

Задача Лицензирование позволяет управлять ключами Kaspersky Endpoint Security.

В этой главе

Добавление активного ключа	116
Добавление дополнительного ключа	116
Удаление активного ключа.....	116
Удаление дополнительного ключа.....	117

Добавление дополнительного ключа

Команда `kesl-control --install-additional-key` добавляет дополнительный ключ. Подробнее о ключах см. в разделе “О лицензионном ключе” на стр. [39](#).

Если активный ключ не добавлен, то дополнительный ключ будет добавлен как основной.

Синтаксис команды

```
kesl-control [-L] --install-additional-key <путь к файлу ключа>
```

Аргументы и ключи

<путь к файлу ключа>

Путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Установить дополнительный ключ из файла `/home/test/00000002.key`:

```
kesl-control --install-additional-key /home/test/00000002.key
```

Удаление активного ключа

Команда `kesl-control --revoke-active-key` удаляет активный ключ.

Синтаксис команды

```
kesl-control [-L] --revoke-active-key
```

Удаление дополнительного ключа

Команда `kesl-control --revoke-additional-key` удаляет дополнительный ключ.

Синтаксис команды

```
kesl-control [-L] --revoke-additional-key
```

Задача Управление хранилищем (Backup ID:10)

В этом разделе содержится информация о задаче Управление хранилищем.

В этой главе

О хранилище	118
Параметры задачи Управление хранилищем	118
Просмотр идентификаторов объектов в хранилище	119
О восстановлении объектов из хранилища	119
Восстановление объектов из хранилища	120
Удаление объектов из хранилища	120

О хранилище

Хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. Резервная копия – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности. Резервные копии могут содержать персональные данные. По умолчанию хранилище расположено в директории `/var/opt/kaspersky/kesl/common/objects-backup/`. Для доступа к заданной по умолчанию директории хранилища требуются root-права.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его вылеченной копии в директорию исходного размещения файла.

Параметры задачи Управление хранилищем

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Управление хранилищем.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

DaysToLive

Интервал времени, в течение которого объекты хранятся в хранилище (в сутках).

Чтобы снять ограничение для времени хранения объектов в хранилище, укажите значение 0.

Значение по умолчанию: 90.

BackupSizeLimit

Максимальный размер хранилища.

При достижении максимального размера хранилища, программа Kaspersky Endpoint Security удаляет самые старые объекты.

Доступные значения:

0 – 999,999 (в мегабайтах).

Чтобы снять ограничение для размера хранилища, укажите значение 0.

Значение по умолчанию: 0.

BackupFolder

Путь к директории хранилища. Вы можете указать в качестве хранилища пользовательскую директорию, отличную от директории, заданной по умолчанию.

В качестве хранилища можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных компьютерах, например смонтированных по протоколам Samba и NFS.

Программа Kaspersky Endpoint Security начинает перемещать объекты в выбранную директорию после изменения параметров и перезапуска Kaspersky Endpoint Security.

Если указанная директория не существует или недоступна, программа Kaspersky Endpoint Security использует директорию хранилища, заданную по умолчанию.

Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-backup/`

Для доступа к заданной по умолчанию директории хранилища требуются root-права.

Просмотр идентификаторов объектов в хранилище

Когда объект помещается в хранилище, программа Kaspersky Endpoint Security присваивает ему числовой идентификатор. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление (см. раздел “Восстановление объектов из хранилища” на стр. [120](#)) или удаление объекта из хранилища (см. раздел “Удаление объектов из хранилища” на стр. [120](#)).

► Чтобы просмотреть идентификаторы объектов в хранилище, выполните следующую команду:

```
kesl-control -B --query
```

Идентификатор объекта будет выведен в строке `ObjectId`.

О восстановлении объектов из хранилища

Программа Kaspersky Endpoint Security хранит объекты в хранилище в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстанавливать объекты из хранилища. Восстановление объектов может потребоваться в следующих случаях:

- При лечении зараженного файла программе Kaspersky Endpoint Security не удалось сохранить его целостность, и в результате информация в файле стала недоступной.
- Если вы считаете, что объект безопасен для сервера, и хотите использовать его, вы можете исключить объект из области проверки, и программа не будет обнаруживать его во время последующих проверок. Для этого вам нужно исключить объект по имени или по названию угрозы,

обнаруженной при выполнении задачи Защита от файловых угроз, а также по имени объекта и по названию угрозы, обнаруженной в задаче антивирусной проверки.

Восстановление зараженных объектов может привести к заражению компьютера.

При восстановлении из хранилища вы можете сохранить файл под другим именем.

Восстановление объектов из хранилища

- ▶ Чтобы восстановить объект из хранилища с исходным именем в исходное местоположение, выполните следующую команду:

```
kesl-control --restore <ID объекта>
```

где ID объекта – это идентификатор объекта в хранилище.

- ▶ Чтобы восстановить объект из хранилища с новым именем в указанную директорию, выполните следующую команду:

```
[-B] --restore <ID объекта> --file <имя и директория файла>
```

Если указанной директории не существует, программа Kaspersky Endpoint Security создает ее.

Удаление объектов из хранилища

- ▶ Чтобы удалить объект из хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove --query "ObjectId == '<ID объекта>'"
```

Пример:

Чтобы удалить объект с ID=15:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

- ▶ Чтобы удалить несколько объектов из хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove --query "<поле><оператор сравнения>  
'<значение>' [и <поле> <оператор сравнения>'<значение>' *]"
```

Пример:

Чтобы удалить объекты в названии которых или в пути к которым содержится "test":

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```


- ▶ *Чтобы удалить все объекты из хранилища, выполните одну из следующих команд:*

```
kesl-control -B --mass-remove
```

или

```
kesl-control -B --mass-remove --query
```

Задача Контроль целостности системы (System_Integrity_Monitoring ID:11)

В этом разделе содержится информация о задаче Контроль целостности системы.

В этой главе

О Контроле целостности системы.....	122
Контроль целостности системы при доступе (OAFIM)	122
Контроль целостности системы по требованию (ODFIM)	123
Параметры задачи Контроль целостности системы при доступе	124
Параметры задачи Контроль целостности системы по требованию	126

О Контроле целостности системы

Задача Контроль целостности системы создана для отслеживания действий, выполняемых с файлами и директориями в области мониторинга, указанной в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом сервере.

Для использования функции контроля целостности системы вам нужно приобрести лицензию, которая включает эту функцию. По умолчанию контроль целостности системы выключен.

Контроль целостности системы может выполняться в режиме реального времени при запуске задачи *Контроль целостности системы при доступе* (OAFIM) (см. раздел “Контроль целостности системы при доступе (OAFIM)” на стр. [122](#)). Кроме этого можно создавать и запускать задачи *Контроль целостности системы по требованию* (ODFIM) (см. стр. [123](#)).

Оба типа задач отправляют уведомления об изменениях в списках контроля доступа к объектам. В случае задачи OAFIM в отчет не включаются данные о том, какие именно изменения внесены. В случае задачи ODFIM в отчет включаются данные об измененных атрибутах и перемещенных файлах и директориях.

Контроль целостности системы при доступе (OAFIM)

Во время работы задачи OAFIM каждое изменение объекта определяется путем перехвата файловых операций в режиме реального времени. При изменении объекта программа Kaspersky Endpoint Security отправляет событие на Сервер администрирования Kaspersky Security Center. Во время работы задачи контрольная сумма файла не рассчитывается. Задача OAFIM не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне *области мониторинга*.

Программа Kaspersky Endpoint Security отслеживает операции с конкретными файлами или в областях, указанных в параметрах задачи.

Области мониторинга

Области мониторинга для задачи Контроль целостности системы всегда должны быть указаны. Администратор может изменять области проверки и мониторинга в режиме реального времени. Если область мониторинга не указана, параметры задачи невозможно сохранить в конфигурационном файле. При добавлении области мониторинга или области исключения программа не проверяет, существует ли такая директория.

Вы можете указать несколько областей мониторинга.

Исключения из области мониторинга

Вы можете создавать исключения из области мониторинга. Исключения указываются для каждой отдельной области и работают только для указанной области мониторинга. Вы можете указать несколько областей исключения.

Исключения имеют более высокий приоритет, чем область мониторинга, и не проверяются задачей, даже если указанная директория или файл находятся в области мониторинга. Если параметры одного из правил указывают область мониторинга на более низком уровне, чем директория, указанная в исключении, область мониторинга не рассматривается при выполнении задачи.

Чтобы указать исключения, можно использовать те же маски в формате командной оболочки, которые используются для указания областей мониторинга.

Контролируемые параметры

Во время работы задачи Контроль целостности системы контролируется изменение следующих параметров:

- содержимое (write (), truncate (), etc.);
- метаданные (правообладание (chmod/chown));
- отметки времени (utimensat);
- расширенные атрибуты (setxattr) и другие.

Технологические ограничения операционной системы Linux не позволяют компоненту Контроль целостности системы определять, какой администратор или процесс внес изменение в файл.

Контроль целостности системы по требованию (ODFIM)

В процессе выполнения задачи ODFIM изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве *снимка состояния системы*.

Вы можете создать несколько задач ODFIM.

Снимок состояния системы

Снимок состояния системы определяется во время первого выполнения задачи ODFIM на компьютере. Для каждой задачи ODFIM создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы относится к области мониторинга. Если снимок состояния системы не соответствует

области мониторинга, программа Kaspersky Endpoint Security создает событие о нарушении целостности системы. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные.

Снимок состояния системы создается заново после завершения задачи ODFIM. Снимок состояния системы также создается при изменении параметров задачи, например, при добавлении новой области мониторинга. При следующем выполнении задачи снимок состояния системы формируется заново.

Вы можете заново создать снимок состояния системы для задачи с помощью соответствующего параметра (см. раздел “Параметры задачи Контроль целостности системы по требованию” на стр. [124](#)).

Задача ODFIM создает хранилище для снимков состояния системы на компьютере с установленным компонентом Контроль целостности системы. По умолчанию снимки состояния системы хранятся в базе данных `/var/opt/kaspersky/kes/private/fim.db`. Для доступа к базе данных, в которой хранятся снимки состояния системы, требуются root-права.

Удалить снимок состояния системы можно, удалив соответствующую задачу ODFIM.

Параметры задачи Контроль целостности системы при доступе

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Контроль целостности системы при доступе.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

UseExcludeMasks

Включает или отключает исключение объектов, указанных параметром `ExcludeMasks` из области мониторинга.

Параметр `UseExcludeMasks` работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

`No` – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: `No`.

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано.

Раздел [ScanScope.item_#]

В разделе `[ScanScope.item_#]` указываются области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга.

Вы можете указать в конфигурационном файле несколько разделов `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

Yes – контролировать указанную область;

No – не контролировать указанную область.

Значение по умолчанию: Yes.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kesl/`.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для мониторинга.

Можно указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (обрабатывать все объекты).

Раздел [ExcludedFromScanScope.item_#]

В разделах `[ExcludedFromScanScope.item_#]` укажите объекты, которые требуется исключить из всех разделов `[ScanScope.item_#]`.

Объекты, удовлетворяющие правилам любого из разделов `[ExcludedFromScanScope.item_#]`, будут исключены из мониторинга. Формат раздела `[ExcludedFromScanScope.item_#]` аналогичен формату раздела `[ScanScope.item_#]`. Вы можете указать в конфигурационном файле несколько разделов `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел `[ExcludedFromScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

Yes – исключать указанные области из мониторинга;

No – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути вы можете использовать маски.

Вы можете использовать символ `*` (звездочка) для формирования маски для имени файла или директории. Один символ `*` можно указать вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir*/file` или `/dir*/*/file`.

Два последовательно идущих символа `*` можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `.`. Например, `/dir**/file*` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir**/**/file` – это неправильная маска.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из мониторинга.

Можно указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (контролировать все объекты).

Параметры задачи Контроль целостности системы по требованию

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Контроль целостности системы по требованию.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

RebuildBaseline

Включает или отключает повторное создание снимка состояния системы после завершения задачи ODFIM.

Доступные значения:

`Yes` – создавать снимок состояния системы повторно после завершения задачи ODFIM.

`No` – не создавать снимок состояния системы повторно после завершения задачи ODFIM.

Значение по умолчанию: `No`.

CheckFileHash

Включает или выключает проверку хеша (SHA-256).

Доступные значения:

`Yes` – включить проверку хеша;

`No` – выключить проверку хеша.

Значение по умолчанию: No.

TrackDirectoryChanges

Включает или выключает мониторинг директорий.

Доступные значения:

Yes – контролировать директории;

No – не контролировать директории.

Значение по умолчанию: No.

TrackLastAccessTime

Включает или выключает проверку времени последнего доступа к файлу. В операционных системах Linux это параметр `noatime`.

Доступные значения:

Yes – проверять время последнего доступа к файлу;

No – не проверять время последнего доступа к файлу.

Значение по умолчанию: No.

UseExcludeMasks

Включает или отключает исключение объектов, указанных параметром `ExcludeMasks` из области мониторинга.

Этот параметр работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

Yes – исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

No – не исключать объекты, указанные в параметре `ExcludeMasks`, из области мониторинга.

Значение по умолчанию: No.

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области мониторинга.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано.

Раздел [ScanScope.item_#]

В разделе `[ScanScope.item_#]` указываются области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга.

Вы можете указать в конфигурационном файле несколько разделов `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области мониторинга.

UseScanArea

Включает или выключает мониторинг указанной области.

Доступные значения:

`Yes` – контролировать указанную область;

`No` – не контролировать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает полный путь к объекту или директориям для мониторинга.

Значение по умолчанию: `/opt/kaspersky/kes1/`.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для мониторинга.

Можно указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: `*` (обрабатывать все объекты).

Раздел `[ExcludedFromScanScope.item_#]`

В разделах `[ExcludedFromScanScope.item_#]` укажите объекты, которые требуется исключить из всех разделов `[ScanScope.item_#]`.

Объекты, удовлетворяющие правилам любого из разделов `[ExcludedFromScanScope.item_#]`, будут исключены из мониторинга. Формат раздела `[ExcludedFromScanScope.item_#]` аналогичен формату раздела `[ScanScope.item_#]`. Вы можете указать в конфигурационном файле несколько разделов `[ExcludedFromScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел `[ExcludedFromScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из мониторинга.

UseScanArea

Указывает, будут ли указанные области исключены из мониторинга.

Доступные значения:

`Yes` – исключать указанные области из мониторинга;

`No` – не исключать указанные области из мониторинга.

Значение по умолчанию: `Yes`.

Path

Указывает путь к объектам или директориям, исключенным из мониторинга. Для указания пути вы можете использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из мониторинга.

Можно указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: * (контролировать все объекты).

Задача Защита от шифрования (AntiCryptor ID:13)

В этом разделе содержится информация о задаче Защита от шифрования.

В этой главе

О задаче Защита от шифрования	130
О блокировке доступа к недоверенным компьютерам	131
Параметры задачи Защита от шифрования	131
Просмотр списка заблокированных компьютеров	134
Разблокировка заблокированных компьютеров	134

О задаче Защита от шифрования

Задача Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

В процессе выполнения задачи Защита от шифрования Kaspersky Endpoint Security проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых директориях защищаемого устройства. Если программа расценивает действия удаленного компьютера, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, она добавляет этот компьютер в список недоверенных устройств и запрещает ему доступ к общим сетевым директориям.

Программа Kaspersky Endpoint Security не расценивает действия как вредоносное шифрование, если обнаруженная активность шифрования имеет место в директориях, исключенных из области задачи Защита от шифрования (см. раздел “Параметры задачи Защита от шифрования” на стр. [131](#)).

По умолчанию программа Kaspersky Endpoint Security блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут.

Для корректной работы задачи Защита от шифрования в операционной системе должна быть установлена хотя бы одна из служб: Samba или NFS. Для службы NFS необходимо, чтобы был установлен пакет rpcbind.

Задача Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP/UDP и IP/IPv6. Работа с протоколами NFS2 и NFS4 не поддерживается. Рекомендуется настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 не использовались для подключения сетевых ресурсов.

Задача Защита от шифрования не блокирует доступ к сетевым файловым ресурсам, пока действия устройства не расцениваются как вредоносные. Таким образом, как минимум один файл будет зашифрован, прежде чем программа обнаружит вредоносную активность.

О блокировке доступа к недоверенным компьютерам

При обнаружении вредоносного шифрования Kaspersky Endpoint Security создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного компьютера. Скомпрометированный компьютер добавляется в список недоверенных компьютеров. Программа Kaspersky Endpoint Security блокирует доступ к общим сетевым директориям для всех удаленных компьютеров в списке недоверенных компьютеров. Информация обо всех заблокированных компьютерах защищаемого сервера отправляется в Kaspersky Security Center.

Правила управления сетевым экраном, созданные задачей Защита от шифрования, невозможно удалить с помощью утилиты iptables: Kaspersky Endpoint Security восстанавливает набор правил раз в минуту. Используйте параметр `--allow-hosts`, чтобы разблокировать компьютер (см. раздел “Разблокировка заблокированных компьютеров” на стр. [134](#)).

По умолчанию Kaspersky Endpoint Security удаляет недоверенные компьютеры из списка через 30 минут после добавления в список. Доступ компьютеров к сетевым файловым ресурсам восстанавливается автоматически после удаления недоверенного компьютера из списка. Вы можете изменять список заблокированных компьютеров и указывать период, после которого заблокированные компьютеры автоматически разблокируются.

Параметры задачи Защита от шифрования

В этом разделе содержится информация о параметрах, которые вы можете указать для задачи Защита от шифрования.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

UseHostBlocker

Включает или выключает блокировку недоверенных компьютеров.

Если блокировка недоверенных компьютеров выключена, Kaspersky Endpoint Security все равно проверяет действия удаленных компьютеров с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда работает задача Защита от шифрования. В случае обнаружения вредоносного шифрования создается событие `EncryptionDetected`, но атакующий компьютер не блокируется.

Доступные значения:

`Yes` – включить блокировку недоверенных компьютеров.

`No` – выключить блокировку недоверенных компьютеров.

Значение по умолчанию: `Yes`.

BlockTime

Указывает длительность блокировки доступа к недоверенному компьютеру в минутах.

Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных компьютеров. Длительность блокирования не является динамическим значением и рассчитывается на момент блокирования.

Доступные значения:

Целое значение от 1 до 4294967295.

Значение по умолчанию: 30

UseExcludeMasks

Включает или отключает исключение объектов, указанных параметром `ExcludeMasks`, из области проверки.

Этот параметр работает, только если указано значение параметра `ExcludeMasks`.

Доступные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`, из области защиты.

`No` – не исключать объекты, указанные параметром `ExcludeMasks`, из области защиты.

Значение по умолчанию: `No`

ExcludeMasks

Указывает список масок, которые определяют объекты, исключаемые из области защиты.

Прежде чем указать этот параметр, убедитесь, что для параметра `UseExcludeMasks` указано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`ExcludeMasks.item_0000`, `ExcludeMasks.item_0001`).

Значение по умолчанию: не задано.

Раздел [ScanScope.item_#]

В разделах `[ScanScope.item_#]` укажите области, которые должна защищать программа Kaspersky Endpoint Security. Для задачи Защита от шифрования должна быть указана минимум одна область защиты. Вы можете указывать только общие директории.

Вы можете указать в конфигурационном файле несколько разделов `[ScanScope.item_#]` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел `[ScanScope.item_#]` содержит следующие параметры:

AreaDesc

Указывает имя области защиты.

Значение по умолчанию: Все папки общего доступа

UseScanArea

Включает или выключает защиту указанной области.

Доступные значения:

`Yes` – защищать указанную область.

`No` – не защищать указанную область.

Значение по умолчанию: `Yes`.

Path

Указывает путь к защищаемым объектам.

Доступные значения:

абсолютный путь, доступный через SMB / NFS (например, Path=/tmp).

AllShared – защищать все ресурсы, доступные через SMB / NFS.

Shared:SMB <путь> – защищать ресурсы, доступные через SMB.

Shared:NFS <путь> – защищать ресурсы, доступные через NFS.

Значение по умолчанию: AllShared.

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты для защиты.

Можно указать несколько элементов AreaMask.item_# в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: * (обрабатывать все объекты).

Раздел [ExcludedFromScanScope.item_#]

В разделах [ExcludedFromScanScope.item_#] укажите объекты, которые требуется исключить из всех разделов [ScanScope.item_#].

Объекты, удовлетворяющие правилам любого из разделов [ExcludedFromScanScope.item_#], не проверяются. Формат раздела [ExcludedFromScanScope.item_#] аналогичен формату раздела [ScanScope.item_#]. Вы можете указать в конфигурационном файле несколько разделов [ExcludedFromScanScope.item_#] в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Каждый раздел [ExcludedFromScanScope.item_#] содержит следующие параметры:

AreaDesc

Указывает имя области, которую нужно исключить из проверки.

Значение по умолчанию: All objects.

UseScanArea

Указывает, будут ли указанные области исключены из защиты.

Доступные значения:

Yes – исключать указанную область из защиты.

No – не исключать указанную область из защиты.

Значение по умолчанию: Yes.

Path

Указывает путь к объектам, исключенным из защиты.

Вы можете указать только абсолютный путь к локальной директории (например, /root/tmp/123), которую не требуется защищать компонентом Защита от шифрования.

Для указания пути можно использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, /dir/*/file или /dir/**/file.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, /dir/**/file*/ или /dir/file**/.

Маску ** можно использовать в имени директории только один раз. Например, /dir/**/**/file – это неправильная маска.

Значение по умолчанию: не задано

AreaMask.item_#

Указывает маску в формате командной оболочки, которая определяет объекты, исключенные из защиты.

Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Kaspersky Endpoint Security будет обрабатывать области по индексу в порядке возрастания.

Значение по умолчанию: * (обрабатывать все объекты).

Просмотр списка заблокированных компьютеров

Вы можете просматривать список недоверенных компьютеров, заблокированных задачей Защита от шифрования.

- *Чтобы просмотреть список заблокированных компьютеров, выполните следующую команду:*

```
kesl-control -H --get-blocked-hosts
```

Будут выведены компьютеры, заблокированные задачей Защита от шифрования.

Разблокировка заблокированных компьютеров

Вы можете вручную разблокировать компьютеры, заблокированные задачей Защита от шифрования, и восстановить сетевой доступ для них.

- *Чтобы разблокировать компьютеры, выполните следующую команду:*

```
kesl-control [-H] --allow-hosts <компьютер>
```

где <компьютер> может быть списком действительных адресов IPv4/IPv6 (включая адреса в короткой форме) или подсетей. Таким образом, вы можете указать компьютеры в виде списка.

Указанные компьютеры будут разблокированы.

Примеры:

Адреса IPv4:

dec - 192.168.0.1
dec - 192.168.0.0/24

Адреса IPv6:

hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::

Задача Защита от веб-угроз (Web_Threat_Protection ID: 14)

В этом разделе содержится информация о задаче Защита от веб-угроз.

В этой главе

О задаче Защита от веб-угроз	136
Параметры задачи Защита от веб-угроз	137

О задаче Защита от веб-угроз

Во время работы задачи Защита от веб-угроз программа Kaspersky Endpoint Security проверяет входящий трафик, не допускает загрузку вредоносных файлов из интернета, а также блокирует фишинговые, рекламные и прочие опасные веб-сайты.

Kaspersky Endpoint Security проверяет трафик, передаваемый по протоколам HTTP, HTTPS и FTP. Также выполняется проверка веб-сайтов и IP-адресов. Вы можете указать определенные сетевые порты или диапазоны сетевых портов для проверки (см. раздел “Параметры сети” на стр. [159](#)).

Для проверки HTTPS-трафика требуется включить проверку защищенных соединений (см. раздел “Параметры сети” на стр. [159](#)). Для проверки FTP-трафика требуется указать параметр `MonitorNetworkPorts=All` (см. раздел “Параметры сети” на стр. [159](#)).

При попытке открытия опасного веб-сайта, Kaspersky Endpoint Security выполняет следующие действия:

- Для HTTP- или FTP-трафика программа блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика – в браузере отображается страница с ошибкой.

При открытии веб-сайта задача Защита от веб-угроз выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных антивирусных баз.
2. Проверяет надежность веб-сайта с помощью эвристического анализа, если он включен (см. раздел “Параметры задачи Защита от веб-угроз” на стр. [137](#)).
3. Проверяет надежность веб-сайта с помощью службы Kaspersky Security Network, если она включена (см. раздел “Включение и выключение использования Kaspersky Security Network” на стр. [163](#)).
Рекомендуется принять участие в Kaspersky Security Network, чтобы увеличить эффективность работы задачи Защита от веб-угроз.
4. Запрещает или разрешает открыть веб-сайт.

Параметры задачи Защита от веб-угроз

В этом разделе описаны параметры задачи Защита от веб-угроз. Задача Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета и блокирует доступ к вредоносным, фишинговым, рекламным и прочим опасным веб-сайтам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ActionOnDetect

Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.

Доступные значения:

Notify – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.

Block – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.

Значение по умолчанию: **Block**.

CheckMalicious

Показывает, выполняется ли проверка ссылок по базе вредоносных веб-адресов.

Доступные значения:

Yes – проверять ссылки на вхождение в базу вредоносных веб-адресов.

No – не проверять ссылки на вхождение в базу вредоносных веб-адресов.

Значение по умолчанию: **Yes**.

CheckPhishing

Показывает, выполняется ли проверка ссылок по базе фишинговых веб-адресов.

Доступные значения:

Yes – проверять ссылки на вхождение в базу фишинговых веб-адресов.

No – не проверять ссылки на вхождение в базу фишинговых веб-адресов.

Значение по умолчанию: **Yes**.

UseHeuristicForPhishing

Показывает, используется ли эвристический анализ для проверки веб-страниц на наличие фишинговых ссылок.

Доступные значения:

Yes – использовать эвристический анализ для обнаружения фишинговых ссылок. Если выбрано это значение, используется поверхностный уровень эвристического анализа – **Light** (наименее тщательная проверка, минимальная загрузка системы). Для задачи Защита от веб-угроз невозможно изменить уровень эвристического анализа.

No – не использовать эвристический анализ для обнаружения фишинговых ссылок.

Значение по умолчанию: **Yes**.

CheckAdware

Показывает, выполняется ли проверка ссылок по базе рекламных веб-адресов.

Доступные значения:

Yes – проверять ссылки на вхождение в базу рекламных веб-адресов.

No – не проверять ссылки на вхождение в базу рекламных веб-адресов.

Значение по умолчанию: No

CheckOther

Показывает, выполняется ли проверка ссылок на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.

Доступные значения:

Yes – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.

No – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные программы, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или персональным данным.

Значение по умолчанию: No

UseTrustedAddresses

Включает или отключает использование списка доверенных веб-адресов. Программа не анализирует информацию, полученную с доверенных веб-адресов, и не проверяет их на вирусы и другие вредоносные объекты. Вы можете указать доверенные веб-адреса с помощью параметра `TrustedAddresses.item_#`.

Доступные значения:

Yes – использовать список доверенных веб-адресов.

No – не использовать список доверенных веб-адресов.

Значение по умолчанию: Yes.

TrustedAddresses.item_#

Доверенные веб-адреса. Для указания веб-адресов вы можете использовать маски.

Вы можете использовать символ * (звездочка) для формирования маски для имени файла или директории. Один символ * можно указать вместо любого набора символов (включая пустой набор), предшествующего символу / в имени файла или директории. Например, `/dir/*/file` или `/dir/**/file`.

Два последовательно идущих символа * можно указать вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/**/file/` или `/dir/file**/`.

Маску ** можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Задача Проверка съемных дисков (Removable_Drives_Scan ID: 16)

В этом разделе содержится информация о задаче Проверка съемных дисков.

В этой главе

О задаче Проверка съемных дисков.....	139
Параметры задачи Проверка съемных дисков	139

О задаче Проверка съемных дисков

Когда запущена задача Проверка съемных дисков, программа проверяет подключенное устройство и его загрузочные секторы на вирусы и вредоносные программы. Выполняется проверка следующих съемных дисков: CD/DVD дисков, Blu-ray дисков, флеш-накопителей (включая USB-модемы), внешних жестких дисков и дискет.

При запуске задачи Проверка съемных дисков программа мониторит подключение съемных дисков к компьютеру. При подключении съемного диска программа запускает задачу проверки загрузочных секторов Boot_Scan (тип BootScan) с параметрами по умолчанию (см. раздел “Параметры задачи проверки загрузочных секторов” на стр. [105](#)). Эту задачу остановить невозможно.

Если вы настроили проверку файлов, программа также запускает одну или несколько задач выборочной проверки Scan_File (тип ODS) (см. раздел “Параметры задачи выборочной проверки” на стр. [97](#)). При необходимости пользователь с правами администратора может остановить выполнение этой задачи.

При изменении параметров задачи Проверка съемных дисков, новые значения не применяются к уже запущенным задачам Scan_File и Boot_Scan.

При остановке задачи Проверка съемных дисков уже запущенные задачи Scan_File и Boot_Scan не останавливаются.

По умолчанию задача Проверка съемных дисков не запущена. При необходимости вы можете запустить или остановить задачу в любой момент (см. раздел “Запуск и остановка задачи” на стр. [74](#)).

Параметры задачи Проверка съемных дисков

В этом разделе описаны параметры задачи Проверка съемных дисков.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanRemovableDrives

Включает или отключает проверку съемных дисков при подключении к компьютеру.

Этот параметр не применяется к CD/DVD-приводам и Blu-ray дискам (см. описание параметра ScanOpticalDrives ниже).

Доступные значения:

DetailedScan – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При детализированной проверке используются параметры по умолчанию задачи проверки по требованию (см. раздел “Параметры задачи выборочной проверки” на стр. [97](#)).

QuickScan – проверять только файлы определенных типов на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). При быстрой проверке используются параметры по умолчанию задачи Защита от файловых угроз (см. раздел “Параметры задачи Защита от файловых угроз” на стр. [80](#)).

NoScan – не проверять съемные диски при подключении.

Значение по умолчанию: **NoScan**.

ScanOpticalDrives

Включает или отключает проверку CD/DVD-приводов и Blu-ray дисков при подключении к компьютеру.

Доступные значения:

DetailedScan – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. При детализированной проверке используются параметры по умолчанию задачи проверки по требованию (см. раздел “Параметры задачи выборочной проверки” на стр. [97](#)).

QuickScan – проверять только файлы определенных типов на CD/DVD-приводах и Blu-ray дисках. При быстрой проверке используются параметры по умолчанию задачи Защита от файловых угроз (см. раздел “Параметры задачи Защита от файловых угроз” на стр. [80](#)).

NoScan – не проверять CD/DVD-приводы и Blu-ray диски при подключении.

Значение по умолчанию: **NoScan**.

BlockDuringScan

Показывает, будут ли при проверке заблокированы файлы на подключенном диске. При проверке загрузочных секторов файлы не блокируются.

Доступные значения:

Yes – блокировать файлы при проверке.

No – не блокировать файлы при проверке.

Значение по умолчанию: **No**

Задача Проверка контейнеров (Container_Scan ID: 18)

В этом разделе содержится информация о задаче Проверка контейнеров.

В этой главе

О задаче Проверка контейнеров	141
Параметры задачи Проверка контейнеров	141
Интеграция с Jenkins	147

О задаче Проверка контейнеров

Во время работы задачи Проверка контейнеров, программа проверяет Docker-контейнеры, образы и пространства имен на вирусы и вредоносные программы. Задача Проверка контейнеров – это однократная полная или выборочная проверка файлов, выполняемая программой Kaspersky Endpoint Security. Вы можете одновременно запустить несколько задач Проверка контейнеров.

По умолчанию задача Проверка контейнеров выключена.

Проверка Docker-контейнеров доступна, если программа активирована по лицензии Kaspersky Hybrid Cloud Security Enterprise.

Параметры задачи Проверка контейнеров

В этом разделе описаны параметры проверки, применяемые к Docker-контейнерам и образам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanContainers

Включает или отключает проверку Docker-контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.

Доступные значения:

`Yes` – проверять Docker-контейнеры, заданные по маске.

`No` – не проверять Docker-контейнеры, заданные по маске.

Значение по умолчанию: `Yes`.

ContainerNameMask

Имя или маска имени проверяемого Docker-контейнера.

Прежде чем указать этот параметр, убедитесь, что для параметра `ScanContainers` выбрано значение `Yes`.

Маски указываются в формате командной оболочки. Можно использовать символы `?` и `*`.

Значения по умолчанию: * (проверять все Docker-контейнеры).

Примеры:

Проверять контейнер с именем my_container:

```
ContainerNameMask=my_container
```

Проверять все контейнеры, имена которых начинаются с my_container:

```
ContainerNameMask=my_container*
```

Проверять все контейнеры, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов:

```
ContainerNameMask=my_?????_container*
```

ScanImages

Включает или отключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра `ImageNameMask`.

Доступные значения:

Yes – проверять образы, заданные по маске.

No – не проверять образы, заданные по маске.

Значение по умолчанию: Yes.

ImageNameMask

Имя или маска имени проверяемых образов.

Прежде чем указать этот параметр, убедитесь, что для параметра `ScanImages` выбрано значение Yes.

Маски указываются в формате командной оболочки. Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (item_xxxx).

Значение по умолчанию: * (проверять все образы).

Примеры:

Проверять образы с именем my_image и значением тега latest:

```
ImageNameMask=my_image:latest
```

Проверять все образы, имена которых начинаются с my_image_, имеющие любое значения тега:

```
ImageNameMask=my_image*
```

DeepScan

Включает или отключает проверку всех слоев образа.

Доступные значения:

Yes – проверять все слои.

No – не проверять все слои.

Значение по умолчанию: No

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри Docker-контейнера описаны ниже.

Доступные значения:

`StopContainerIfFailed` – программа останавливает Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – программа останавливает Docker-контейнер при обнаружении зараженного объекта.

`Skip` – программа не выполняет никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`.

ImageAction

Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.

Доступные значения:

`Skip` – программа не выполняет никаких действий над образами при обнаружении зараженного объекта.

`Delete` – программа удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные Docker-контейнеры будут остановлены, а затем удалены.

Значение по умолчанию: `Skip`.

Параметры проверки

Описанные ниже параметры применяются к объектам внутри Docker-контейнеров и образов.

ScanArchived

Включает или отключает проверку архивов, включая самораспаковывающиеся архивы (SFX-архивы). Kaspersky Endpoint Security обнаруживает зараженные объекты в архивах, но не лечит их.

Доступные значения:

`Yes` – проверять архивы, включая самораспаковывающиеся архивы (SFX-архивы). Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

`No` – не проверять архивы.

Значение по умолчанию: `Yes`.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

`Yes` – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: Yes.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.

Доступные значения:

Yes – проверять почтовые базы.

No – не проверять почтовые базы.

Значение по умолчанию: No.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: No.

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров программы Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

Idle – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

Normal – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: Idle.

TimeLimit

Продолжительность проверки отдельного архива (в секундах). Программа пропускает архивы, проверка которых выполняется дольше указанного времени.

Доступные значения:

0 – 9999

Если указано значение 0, продолжительность проверки не ограничена.

Значение по умолчанию: 0

SizeLimit

Максимальный размер проверяемого архива (в мегабайтах). Если архив больше указанного значения, программа пропускает его при проверке.

Доступные значения:

0 – 999999

Если указано значение 0, выполняется проверка архивов любого размера.

Значение по умолчанию: 0

Каждому обнаруженному объекту присваивается статус, показывающий его опасность для системы. Вы можете выбрать два действия, которые программа будет выполнять над зараженными объектами. Сначала программа пытается выполнить первое действие над зараженным объектом. Если выполнить первое действие не удалось, выполняется второе действие.

Указанные действия выполняются на том уровне, на котором был обнаружен зараженный объект.

FirstAction

Первое действие, выполняемое над зараженным объектом. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие `Remove`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами “Лаборатории Касперского”.

`Skip` – программа пропускает зараженный объект при проверке.

Значение по умолчанию: `Recommended`.

SecondAction

Действие, выполняемое над зараженным объектом, если не удалось выполнить действие, заданное параметром `FirstAction`.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами “Лаборатории Касперского”.

`Skip` – программа блокирует доступ к зараженному объекту.

Значение по умолчанию: `Skip`.

UseExcludeMasks

Включает или отключает исключение объектов из проверки.

Доступные значения:

`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать из проверки объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: No.

UseExcludeThreats

Включает или отключает исключение из проверки заданных угроз.

Доступные значения:

Yes – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

No – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: No.

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, относительно которых во время проверки программа приняла решение “чистые”.

Доступные значения:

Yes – записывать в журнал информацию о “чистых” объектах. Не рекомендуется надолго устанавливать значение *Yes* для этого параметра, так как запись большого объема информации может снизить производительность программы.

No – не записывать в журнал информацию о “чистых” объектах.

Значение по умолчанию: No.

ReportPackedObjects

Включает или отключает запись в журнал информации об объектах, которые являются частью составных объектов.

Доступные значения:

Yes – записывать в журнал информацию об упакованных объектах. Не рекомендуется надолго устанавливать значение *Yes* для этого параметра, так как запись большого объема информации может снизить производительность программы.

No – не записывать в журнал информацию о упакованных объектах.

Значение по умолчанию: No.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

Yes – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение *Yes* для этого параметра, так как запись большого объема информации может снизить производительность программы.

No – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: No.

UseAnalyzer

Включает или отключает эвристический анализатор.

Доступные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Уровень эвристического анализа.

Доступные значения:

Light – наименее детализированная проверка, минимальная нагрузка на систему.

Medium – средняя детализация при проверке, сбалансированная нагрузка на систему.

Deep – наиболее детализированная проверка, максимальная нагрузка на систему.

Recommended – оптимальный уровень, рекомендуемый специалистами “Лаборатории Касперского”.

Значение по умолчанию: Recommended.

UseIChecker

Включает или отключает использование технологии iChecker при проверке.

Доступные значения:

Yes – использовать технологию iChecker при проверке.

No – не использовать технологию iChecker при проверке.

Значение по умолчанию: Yes.

Интеграция с Jenkins

Программа Kaspersky Endpoint Security поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для проверки Docker-образов на разных этапах. Например, можно проверять Docker-образы в репозитории в процессе разработки или перед публикацией.

► Для интеграции Kaspersky Endpoint Security с Jenkins выполните следующие действия:

1. Установите Docker Engine на узле Jenkins.

Дополнительная информация приведена в документации Docker Engine (<https://docs.docker.com/install/>).

2. Предоставьте пользователю Jenkins права администратора Kaspersky Endpoint Security:

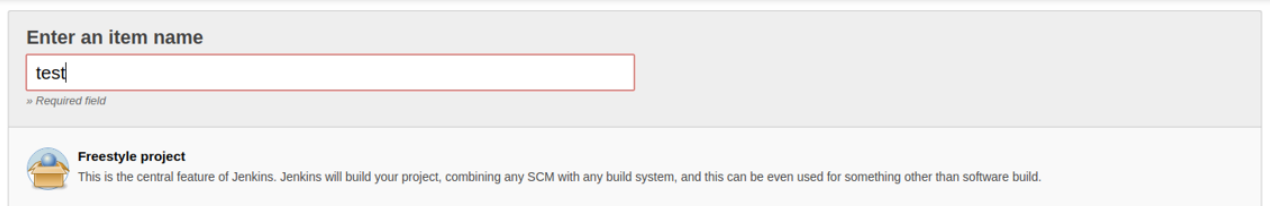
```
kesl-control --grant-role admin <имя пользователя Jenkins>
```

3. Добавьте пользователя Jenkins в группу docker:

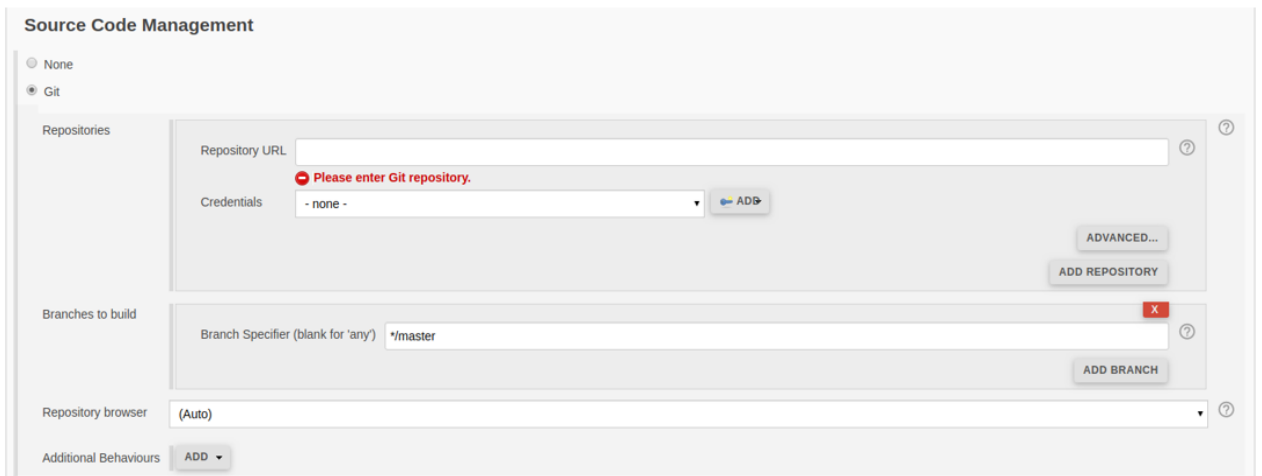
```
sudo usermod -aG docker <имя пользователя Jenkins>
```

Обычно используется имя jenkins.

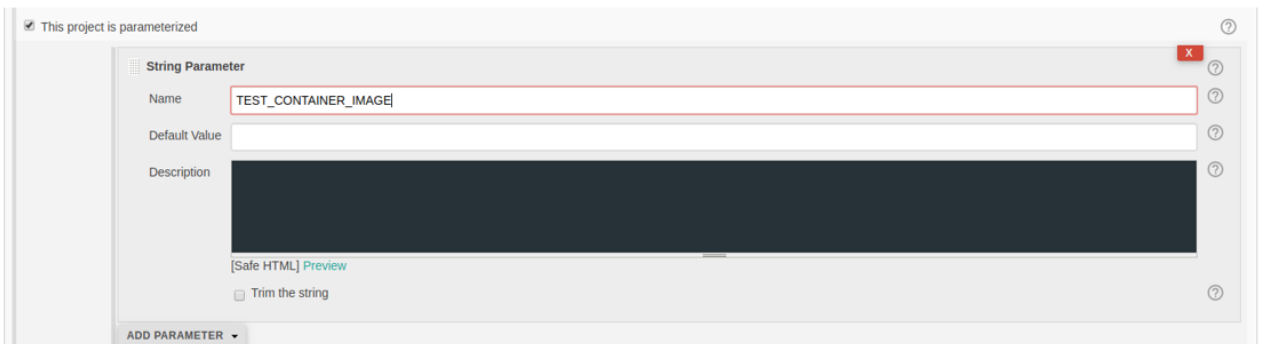
- В Jenkins создайте новое задание на сборку с название `test` (**Создать элемент** → **Указать название элемента**).



- Укажите репозиторий Git для вашего проекта.



- В параметрах задания на сборку добавьте название Docker-образа (строковый параметр), например, `TEST_CONTAINER_IMAGE`.



- В поле **Команда** введите скрипт shell, чтобы выполнить проверку Docker-образа:

```
echo "Проверка Docker-образа"
CONTAINER_ID=`/opt/kaspersky/kesl/bin/kesl-control --scan-
container ${TEST_CONTAINER_IMAGE}`
echo "Тест"
```

```
echo "Удаление контейнера"
```

```
docker rm -f $CONTAINER_ID
```

- Чтобы выполнить проверку Docker-образа, выполните следующий скрипт:

```
echo "Проверка Docker-образа "
```

```
SCAN_RESULT=$( /opt/kaspersky/kesl/bin/kesl-control --scan-
container ${TEST_IMAGE_NAME}*)
```

```
echo "Проверка выполнена: "
echo $SCAN_RESULT
```



9. Чтобы выполнить проверку Docker-образа из репозитория, выполните следующий скрипт:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-
dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
```

```
echo "Собрать образ из ${DOCKER_FILE}"
```

```
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
    echo "Docker-файл получен: ${DOCKER_FILE_FETCHED}"
else
    echo "Docker-файл не получен"
    exit 1
fi
```

```
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME} .
```

```
echo "Проверка Docker-образа"
SCAN_RESULT=$( /opt/kaspersky/kesl/bin/kesl-control --scan-
container ${TEST_IMAGE_NAME}*)
```

```
echo "Проверка выполнена: "
echo $SCAN_RESULT
```

10. Сохраните задание на сборку.

Задача Выборочная проверка контейнеров (Container_Scan ID: 19)

В этом разделе содержится информация о задаче Выборочная проверка контейнеров.

В этой главе

О задаче Выборочная проверка контейнеров.....	150
Параметры задачи Выроверборочная проверка контейнеров	150
Запуск задачи Выборочная проверка контейнеров	157

О задаче Выборочная проверка контейнеров

Задача Выборочная проверка контейнеров служит для хранения параметров, применяемых командой `kesl-control --scan-container`. Эта задача не является пользовательской, вы не можете удалить ее.

Вы можете проверить Docker-контейнер или образ с помощью следующей команды:

```
kesl-control --scan-container <имя Docker-контейнера или образа>
```

Программа создает временную задачу антивирусной проверки контейнеров (тип ContainerScan) (см. раздел “Задача Проверка контейнеров (Container_Scan ID: 18)” на стр. [141](#)) с параметрами задачи Custom_Container_Scan. После завершения проверки временная задача автоматически удаляется.

Вы можете изменить параметры проверки для временной задачи Custom_Container_Scan из командной строки.

При создании пользовательской задачи Проверки контейнеров с помощью команды `kesl-control --create-task <имя задачи> --type ContainerScan` программа Kaspersky Endpoint Security использует значения параметров по умолчанию задачи Проверка контейнеров (см. раздел “Параметры задачи Проверка контейнеров” на стр. [141](#)), за исключением параметра `ScanPriority=Normal`.

Примеры:

Проверить Docker-контейнер с именем `my_container`:

```
kesl-control --scan-container my_container
```

Проверить Docker-образ с именем `my_image` (все теги):

```
kesl-control --scan-container my_image*
```

Параметры задачи Выборочная проверка контейнеров

В этом разделе описаны параметры проверки, применяемые к Docker-контейнерам и образам.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

ScanContainers

Включает или отключает проверку Docker-контейнеров, заданных по маске. Маски можно указывать с помощью параметра `ContainerNameMask`.

Доступные значения:

`Yes` – проверять Docker-контейнеры, заданные по маске.

`No` – не проверять Docker-контейнеры, заданные по маске.

Значение по умолчанию: `Yes`.

ContainerNameMask

Имя или маска имени проверяемого Docker-контейнера. Прежде чем указать этот параметр, убедитесь, что для параметра `ScanContainers` выбрано значение `Yes`.

Маски указываются в формате командной оболочки. Можно использовать символы `?` и `*`.

Значения по умолчанию: `*` (проверять все Docker-контейнеры).

Примеры:

Проверять контейнер с именем `my_container`:

```
ContainerNameMask=my_container
```

Проверять все контейнеры, имена которых начинаются с `my_container`:

```
ContainerNameMask=my_container*
```

Проверять все контейнеры, имена которых начинаются с `my_`, затем содержат пять любых символов, затем слово `_container` и заканчиваются любой последовательностью символов:

```
ContainerNameMask=my_?????_container*
```

ScanImages

Включает или отключает проверку образов, заданных по маске. Маски можно указывать с помощью параметра `ImageNameMask`.

Доступные значения:

`Yes` – проверять образы, заданные по маске.

`No` – не проверять образы, заданные по маске.

Значение по умолчанию: `Yes`.

ImageNameMask

Имя или маска имени проверяемых образов. Прежде чем указать этот параметр, убедитесь, что для параметра `ScanImages` выбрано значение `Yes`.

Маски указываются в формате командной оболочки.

Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом (`item_xxxx`).

Значение по умолчанию: `*` (проверять все образы).

Примеры:

Проверять образы с именем `my_image` и значением тега `latest`:

```
ImageNameMask=my_image:latest
```

Проверять все образы, имена которых начинаются с `my_image_`, имеющие любое значения тега:

```
ImageNameMask=my_image*
```

DeepScan

Включает или отключает проверку всех слоев образа.

Доступные значения:

`Yes` – проверять все слои.

`No` – не проверять все слои.

Значение по умолчанию: `No`.

ContainerScanAction

Действие над Docker-контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри Docker-контейнера описаны ниже, в разделе **Параметры проверки**.

Доступные значения:

`StopContainerIfFailed` – программа останавливает Docker-контейнер, если не удалось вылечить зараженный объект.

`StopContainer` – программа останавливает Docker-контейнер при обнаружении зараженного объекта.

`Skip` – программа не выполняет никаких действий над Docker-контейнерами при обнаружении зараженного объекта.

Значение по умолчанию: `StopContainerIfFailed`.

ImageAction

Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже, в разделе **Параметры проверки**.

Доступные значения:

`Skip` – программа не выполняет никаких действий над образами при обнаружении зараженного объекта.

`Delete` – программа удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные Docker-контейнеры будут остановлены, а затем удалены.

Значение по умолчанию: `Skip`.

Параметры проверки

Описанные ниже параметры применяются к объектам внутри Docker-контейнеров и образов.

ScanArchived

Включает или отключает проверку архивов, включая самораспаковывающиеся архивы (SFX-архивы). Kaspersky Endpoint Security обнаруживает зараженные объекты в архивах, но не лечит их.

Доступные значения:

Yes – проверять архивы, включая самораспаковывающиеся архивы (SFX-архивы). Если указано значение `FirstAction=Recommended`, программа удаляет архив, содержащий угрозу.

No – не проверять архивы.

Значение по умолчанию: **Yes**.

ScanSfxArchived

Включение или отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Доступные значения:

Yes – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значение по умолчанию: **Yes**.

ScanMailBases

Включение или отключение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.

Доступные значения:

Yes – проверять почтовые базы.

No – не проверять почтовые базы.

Значение по умолчанию: **No**.

ScanPlainMail

Включение или отключение проверки сообщений электронной почты в текстовом формате (plain text).

Доступные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: **No**.

ScanPriority

Приоритет задачи. Приоритет задачи проверки – это параметр, сочетающий несколько внутренних параметров Kaspersky Endpoint Security и параметров запуска процесса. С помощью этого параметра можно указать, как программа распределяет ресурсы системы для запущенных задач.

Доступные значения:

Idle – запустить задачу проверки с низким приоритетом. Выберите это значение, чтобы выделить ресурсы программы на выполнение других задач, включая процессы пользователей. Выполнение текущей задачи займет больше времени.

`Normal` – запустить задачу проверки со стандартным приоритетом. Выберите это значение, чтобы текущая задача выполнялась быстрее.

Значение по умолчанию: `Normal`.

TimeLimit

Продолжительность проверки отдельного архива (в секундах). Программа пропускает архивы, проверка которых выполняется дольше указанного времени.

Доступные значения:

0 – 9999

Если указано значение 0, продолжительность проверки не ограничена.

Значение по умолчанию: 0

SizeLimit

Максимальный размер проверяемого архива (в мегабайтах).

Если архив больше указанного значения, программа пропускает его при проверке.

Доступные значения:

0 – 999999

Если указано значение 0, выполняется проверка архивов любого размера.

Значение по умолчанию: 0

Каждому обнаруженному объекту присваивается статус, показывающий его опасность для системы. Вы можете выбрать два действия, которые программа будет выполнять над зараженными объектами. Сначала программа пытается выполнить первое действие над зараженным объектом. Если выполнить первое действие не удалось, выполняется второе действие.

Указанные действия выполняются на том уровне, на котором был обнаружен зараженный объект.

FirstAction

Первое действие, выполняемое над зараженным объектом. Если зараженный объект обнаружен в файле, обращение к которому происходит по символической ссылке, входящей в область проверки (в то время как сам файл, обращение к которому происходит по символической ссылке, не входит в область проверки), над этим файлом будет выполнено указанное действие. Например, если выбрано действие `Remove`, программа удалит файл, но символическая ссылка останется и будет ссылаться на несуществующий файл.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами “Лаборатории Касперского”.

`Skip` – программа пропускает зараженный объект при проверке.

Значение по умолчанию: `Recommended`.

SecondAction

Действие, выполняемое над зараженным объектом, если не удалось выполнить действие, заданное параметром `FirstAction`.

Доступные значения:

`Disinfect` – программа блокирует доступ к зараженному объекту и пытается его вылечить.

`Remove` – программа блокирует доступ к зараженному объекту и удаляет его.

`Recommended` – программа выполняет действие, рекомендованное специалистами “Лаборатории Касперского”.

`Skip` – программа блокирует доступ к зараженному объекту.

Значение по умолчанию: `Skip`.

UseExcludeMasks

Включает или отключает исключение объектов из проверки.

Доступные значения:

`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks`.

`No` – не исключать из проверки объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

UseExcludeThreats

Включает или отключает исключение из проверки заданных угроз.

Доступные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ReportCleanObjects

Включает или отключает запись в журнал информации о проверенных объектах, которым программа во время проверки присвоила статус “чистые”.

Доступные значения:

`Yes` – записывать в журнал информацию о “чистых” объектах. Не рекомендуется надолго устанавливать значение `Yes` для этого параметра, так как запись большого объема информации может снизить производительность программы.

`No` – не записывать в журнал информацию о “чистых” объектах.

Значение по умолчанию: `No`.

ReportPackedObjects

Включает или отключает запись в журнал информации об объектах, которые являются частью составных объектов.

Доступные значения:

Yes – записывать в журнал информацию об упакованных объектах. Не рекомендуется надолго устанавливать значение *Yes* для этого параметра, так как запись большого объема информации может снизить производительность программы.

No – не записывать в журнал информацию о упакованных объектах.

Значение по умолчанию: *No*.

ReportUnprocessedObjects

Включает или отключает запись в журнал информации о файлах, которые по какой-то причине не были обработаны.

Доступные значения:

Yes – записывать в журнал информацию о непроверенных объектах. Не рекомендуется надолго устанавливать значение *Yes* для этого параметра, так как запись большого объема информации может снизить производительность программы.

No – не записывать в журнал информацию о необработанных объектах.

Значение по умолчанию: *No*.

UseAnalyzer

Включает или отключает эвристический анализатор.

Доступные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: *Yes*.

HeuristicLevel

Уровень эвристического анализа.

Доступные значения:

Light – наименее детализированная проверка, минимальная нагрузка на систему.

Medium – средняя детализация при проверке, сбалансированная нагрузка на систему.

Deep – наиболее детализированная проверка, максимальная нагрузка на систему.

Recommended – оптимальный уровень, рекомендуемый специалистами “Лаборатории Касперского”.

Значение по умолчанию: *Recommended*.

UseIChecker

Включает или отключает использование технологии iChecker при проверке.

Доступные значения:

Yes – использовать технологию iChecker при проверке.

No – не использовать технологию iChecker при проверке.

Значение по умолчанию: *Yes*.

Запуск задачи Выборочная проверка контейнеров

- ▶ Чтобы запустить задачу Выборочная проверка контейнеров, выполните следующую команду:

```
kesl-control --scan-container <ID Docker-контейнера или образа|имя Docker-контейнера|имя образа[:тег]>
```

Если существует несколько элементов с одинаковым именем, программа проверяет их все.

Задача Анализ поведения (Behavior_Detection ID: 20)

В этом разделе содержится информация о задаче Анализ поведения.

Задача Анализ поведения контролирует вредоносную активность в операционной системе. При обнаружении вредоносной активности программа Kaspersky Endpoint Security завершает этот процесс.

По умолчанию задача запускается при старте программы Kaspersky Endpoint Security. Задачу Анализ поведения можно запустить или остановить (см. раздел “Запуск и остановка задачи” на стр. [74](#)).

Задача Анализ поведения не имеет параметров.

Проверка зашифрованных соединений

В этом разделе содержится информация о параметрах проверки зашифрованных соединений.

В этой главе

Параметры сети	159
Управление параметрами проверки зашифрованных соединений	161

Параметры сети

В этом разделе описаны параметры проверки зашифрованных соединений. Эти параметры применяются в задачах Защита от веб-угроз (см. раздел “О задаче Защита от веб-угроз” на стр. [136](#)) и Защита от сетевых угроз.

В сертифицированной версии программы задача Защита от сетевых угроз недоступна.

Ниже описаны все доступные значения и значения по умолчанию для каждого параметра.

EncryptedConnectionsScan

Включает или отключает проверку зашифрованного трафика. Для FTP протокола проверка зашифрованных соединений по умолчанию отключена.

Доступные значения:

`Yes` – включить проверку зашифрованных соединений.

`No` – выключить проверку зашифрованных соединений. Программа не расшифровывает зашифрованный трафик.

Значение по умолчанию: `Yes`.

EncryptedConnectionsScanErrorAction

Действие, выполняемое программой при возникновении ошибки проверки зашифрованного соединения на веб-сайте.

Доступные значения:

`AddToAutoExclusions` – добавить домен, на котором возникла ошибка, в список доменов с ошибками проверки. Программа не будет контролировать зашифрованный сетевой трафик при посещении этого домена.

`Disconnect` – заблокировать сетевое соединение.

Значение по умолчанию: `AddToAutoExclusions`.

CertificateVerificationPolicy

Задаёт способ проверки сертификатов программой Kaspersky Endpoint Security.

Если сертификат является самозаверяющим, программа не выполняет дополнительную проверку.

Доступные значения:

`FullCheck` – программа использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.

`LocalCheck` – программа не использует интернет для проверки сертификата.

Значение по умолчанию: `FullCheck`.

UntrustedCertificateAction

Действие, выполняемое программой при возникновении ошибки проверки зашифрованного соединения на веб-сайте.

Доступные значения:

`Allow` – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.

`Block` – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.

Значение по умолчанию: `Allow`.

ManageExclusions

Включает или отключает использование исключений при проверке зашифрованного трафика.

Доступные значения:

`Yes` – не проверять веб-сайты, указанные в разделе `[Exclusions.item_#]`.

`No` – проверять все веб-сайты.

Значение по умолчанию: `No`.

MonitorNetworkPorts

Способ контроля сетевых портов программой Kaspersky Endpoint Security.

Доступные значения:

`Selected` – контролировать только сетевые порты, указанные в разделе `[NetworkPorts.item_#]` (см. ниже).

`All` – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.

Значение по умолчанию: `Selected`.

Раздел [Exclusions.item_#]

В разделе `[Exclusions.item_#]` указаны домены, исключенные из проверки. Программа не проверяет зашифрованные соединения, установленные при посещении указанных доменов.

DomainName

Имя домена. Для указания домена можно использовать маски.

Раздел [NetworkPorts.item_#]

В разделе `[NetworkPorts.item_#]` указаны сетевые порты, контролируемые программой.

PortName

Описание сетевого порта.

Port

Номера сетевых портов, контролируемые программой.

Доступные значения:

1 - 65535

Управление параметрами проверки зашифрованных соединений

Из командной строки можно управлять параметрами проверки зашифрованных соединений.

- ▶ Чтобы вывести список исключений из проверки зашифрованных соединений, добавленных пользователем, выполните следующую команду:

```
kesl-control -N --query user
```

- ▶ Чтобы вывести список исключений из проверки зашифрованных соединений, добавленных Kaspersky Endpoint Security, выполните следующую команду:

```
kesl-control -N --query auto
```

- ▶ Чтобы вывести список исключений из проверки зашифрованных соединений, полученных из баз “Лаборатории Касперского”, выполните следующую команду:

```
kesl-control -N --query kl
```

- ▶ Чтобы очистить список доменов, которые программа Kaspersky Endpoint Security автоматически исключила из проверки, выполните следующую команду:

```
kesl-control -N --clear-web-auto-excluded
```

- ▶ Чтобы выгрузить параметры проверки зашифрованных соединений из хранилища, выполните следующую команду:

```
kesl-control [-N] [--get-net-settings] [--file <имя и путь к файлу>]
```

Выходной файл имеет формат INI.

- ▶ Чтобы сохранить параметры проверки зашифрованных соединений в файл, выполните следующую команду:

```
kesl-control [-N] [--set-net-settings] [--file <имя и путь к файлу>]
```

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

В этой главе

Об участии в Kaspersky Security Network.....	162
Включение и выключение использования Kaspersky Security Network.....	163
Проверка подключения к Kaspersky Security Network.....	164
Дополнительная защита с использованием Kaspersky Security Network	164

Об участии в Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний “Лаборатории Касперского” о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают:

- Глобальный KSN – инфраструктура расположена на серверах “Лаборатории Касперского”.
- Локальный KSN (Kaspersky Private Security Network) – инфраструктура расположена на сторонних серверах поставщика услуг, например, внутри сети интернет-провайдера.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

При использовании Локального KSN статистическая информация и файлы с компьютеров, на которых установлена программа Kaspersky Endpoint Security, не отправляются на серверы “Лаборатории Касперского”.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

Участие пользователей в Kaspersky Security Network позволяет “Лаборатории Касперского” разрабатывать решения для нейтрализации угроз и уменьшать количество ложных срабатываний компонентов программы.

Существует два варианта участия в Kaspersky Security Network:

- **Kaspersky Security Network со статистикой** – вы можете получать информацию из базы знаний. Программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в “Лабораторию Касперского” для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.
- **Kaspersky Security Network без статистики** – вы можете получать информацию из базы знаний, но программа не отправляет анонимную статистику и данные о типах и источниках угроз.

Сбор, обработка и хранение персональных данных пользователя не производится. Более подробная информация об отправке в “Лабораторию Касперского”, хранении и уничтожении статистических данных, полученных во время использования KSN, приведена в Положении о Kaspersky Security Network и на веб-сайте “Лаборатории Касперского” (<https://www.kaspersky.ru/products-and-services-privacy-policy>). Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network входит в комплект поставки программы и находится в директории /opt/kaspersky/kesl/doc/.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы ksnproху.

Служба ksnproху предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба ksnproху кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробная информация о службе ksnproху приведена в документации Kaspersky Security Center <https://help.kaspersky.com/KSC/11/ru-RU/5022.htm>.

Участие в Kaspersky Security Network является добровольным. Kaspersky Endpoint Security предлагает принять участие в KSN во время первоначальной настройки программы. Вы можете начать или прекратить использование KSN в любой момент.

Включение и выключение использования Kaspersky Security Network

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

► Чтобы включить использование Kaspersky Security Network, выполните одну из следующих команд:

- Чтобы включить использование Kaspersky Security Network со статистикой, выполните команду:

```
kesl-control --set-app-settings UseKSN=Extended
```

- Чтобы включить использование Kaspersky Security Network без статистики, выполните команду:

```
kesl-control --set-app-settings UseKSN=Basic
```

- ▶ Чтобы выключить использование Kaspersky Security Network, выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=No
```

- ▶ Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:

```
kesl-control --set-app-settings --file <имя конфигурационного файла>
```

Если программа Kaspersky Endpoint Security, установленная на компьютере, работает под управлением политики, которая была назначена в Kaspersky Security Center, значение параметра `UseKSN` можно изменить только в Kaspersky Security Center.

Если программа Kaspersky Endpoint Security, установленная на компьютере, прекратила работать под управлением политики, параметру присваивается следующее значение: `UseKSN=No`.

Проверка подключения к Kaspersky Security Network

- ▶ Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

```
kesl-control --app-info
```

Строка `KSN state` показывает статус подключения к Kaspersky Security Network:

- Если отображается статус `Extended`, программа Kaspersky Endpoint Security подключена к Kaspersky Security Network, информация из базы знаний доступна, отправляются анонимная статистика и данные о типах и источниках угроз.
- Если отображается статус `Basic`, программа Kaspersky Endpoint Security подключена к Kaspersky Security Network, информация из базы знаний доступна, но анонимная статистика и данные о типах и источниках угроз не отправляются.
- Если отображается статус `No`, программа Kaspersky Endpoint Security не подключена к Kaspersky Security Network.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN. При использовании Локального KSN в строке `KSN state` отображается статус `Basic`.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Вы не участвуете в Kaspersky Security Network.
- Программа не активирована, или срок действия лицензии истек.
- Выявлены проблемы, связанные с ключом. Например, ключ попал в черный список ключей.

События и отчеты

Во время работы Kaspersky Endpoint Security возникают события, отражающие изменение состояния антивирусной защиты сервера и состояния Kaspersky Endpoint Security в целом.

Для просмотра событий Kaspersky Endpoint Security из командной строки используйте команды управления журналом событий или команду `kesl-control -W`.

Вы можете своевременно получать информацию о событиях с помощью уведомлений. *Уведомление* – это сообщение с информацией о событии, которое произошло во время работы программы. Вы можете настроить уведомление администратора о событиях по электронной почте через Kaspersky Security Center.

Подробную информацию о событиях и уведомлениях Kaspersky Security Center см. в документации Kaspersky Security Center (<https://help.kaspersky.com/KSC/11/ru-RU/5022.htm>).

Об отчетах

Информация о работе каждого компонента Kaspersky Endpoint Security, результаты выполнения каждой задачи и работы всей программы в целом записываются в отчеты.

Способы формирования отчетов различаются и зависят от параметров программы Kaspersky Endpoint Security и использования Kaspersky Security Center.

- Все отчеты хранятся в локальном хранилище событий программы. Хранилище событий расположено в директории, указанной в параметре программы `EventsStoragePath` (см. раздел “Общие параметры Kaspersky Endpoint Security” на стр. [52](#)). По умолчанию, программа сохраняет данные о событиях в файл базы данных `/var/opt/kaspersky/kesl/events.db`. Для доступа к базе данных событий требуются root-права.
- Если управление программой Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Информация об управлении отчетами в Kaspersky Security Center приведена в документации Kaspersky Security Center (<https://help.kaspersky.com/KSC/11/ru-RU/5022.htm>).
- Если для параметра программы `UseSyslog` задано значение `UseSyslog=Yes` (см. раздел “Общие параметры Kaspersky Endpoint Security” на стр. [52](#)), данные о событиях также записываются в `syslog`. Для доступа к `syslog` требуются root-права.

В отчетах могут содержаться следующие персональные данные пользователей:

- имя и идентификатор пользователя в операционной системе;
- путь к файлам пользователя;
- IP-адреса удаленных компьютеров, проверяемых задачей Защита от шифрования (см. раздел “Задача Защита от шифрования (AntiCryptor ID:13)” на стр. [130](#));
- IP-адреса отправителей и получателей сетевых пакетов, проверяемых задачей Управление сетевым экраном;
- веб-адреса источников обновлений (см. раздел “Об источниках обновлений” на стр. [111](#));
- общие параметры программы (см. раздел “Общие параметры Kaspersky Endpoint Security” на стр. [52](#));
- названия и параметры задач;

- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя;
- названия Docker-контейнеров и образов;
- пути к Docker-контейнерам и образам;
- названия и идентификаторы устройств.

Включение вывода событий

Команда `kesl-control -W` включает вывод событий Kaspersky Endpoint Security. Вы можете использовать эту команду либо отдельно для вывода всех событий программы Kaspersky Endpoint Security, либо вместе с командой `kesl-control --start-task` для вывода событий, связанных только с запущенной задачей. Для вывода только определенных событий вы можете использовать команду `--query` с флагом `-W`.

Команда возвращает название события и дополнительную информацию о событии.

Синтаксис команды

```
kesl-control -W
```

Пример:

Включить режим вывода событий Kaspersky Endpoint Security:

```
kesl-control -W
```

Просмотр журнала событий в командной строке

Вы можете просмотреть события программы с помощью команд управления журналом событий.

Синтаксис команды

```
kesl-control [-E] --query "<поле><оператор сравнения> '<значение>' [и <поле>  
<оператор сравнения>'<значение>' ]* ] --limit --offset --file <имя файла и  
путь> --db <файл БД>
```

Аргументы и ключи

`--query`

Вывод информации о событиях, удовлетворяющих фильтру.

`--limit`

Максимальное количество событий, о которых выводится информация

`--offset`

Количество записей, на которое следует отступить от начала выборки.

`--file <имя файла и путь>`

Имя файла для вывода событий и путь к нему

--db <файл БД>

Имя файла базы данных.

Просмотр событий в Kaspersky Security Center

► Чтобы посмотреть список всех событий в работе Сервера администрирования Kaspersky Security Center, управляемых устройств и программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В рабочей области узла **Сервер администрирования** перейдите на закладку **События**.

В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **Выборки событий**. События в списке не обновляются автоматически. Чтобы просмотреть последние события, обновите список по ссылке **Обновить**.

В Kaspersky Security Center вы можете выполнять следующие действия при просмотре событий:

- Выбирать выборку, события из которой должны отображаться в списке. Раскрывающийся список **Выборки событий** содержит predefined выборки (созданные по умолчанию), а также пользовательские выборки. Если пользователь не создавал собственные выборки, пользовательских выборок нет в списке.
- Добавлять или удалять графы из списка событий.
- Искать события в списке по ключевым словам.
- Просматривать подробную информацию о событии, выбранном в списке. Поле с подробной информацией о событии находится справа от списка событий.
- Создавать и настраивать выборки событий.
- Экспортировать и импортировать события выборки.
- Настраивать уведомления о событиях и экспорт событий в SIEM-систему.

Подробную информацию о работе с событиями см. в документации Kaspersky Security Center.

Проверка целостности компонентов программы

Программа Kaspersky Endpoint Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько исполняемых модулей или файлов программы другими файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов программы, в Kaspersky Endpoint Security 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.

Проверка целостности компонентов программы выполняется с помощью утилиты `integrity_check_tool`, расположенной в директории `/opt/kaspersky/kesl/bin`. Утилита проверяет целостность *файла манифеста*, содержащего список файлов программы, целостность которых важна для корректной работы компонентов программы.

Файл манифеста `integrity_check.xml`, защищенный криптографической сигнатурой “Лаборатории Касперского”, расположен в той же директории, где утилита проверки целостности (`/opt/kaspersky/kesl/bin`).

Для запуска утилиты проверки целостности требуется учетная запись с root-правами.

Проверку целостности можно выполнять с помощью утилиты, поставляемой вместе с программой, или с помощью утилиты, расположенной на сертифицированном компакт-диске.

Рекомендуется запускать утилиту проверки целостности с сертифицированного компакт-диска, чтобы гарантировать целостность самой утилиты. При запуске утилиты с компакт-диска требуется указать полный путь к файлу манифеста в директории программы.

► Чтобы проверить целостность компонентов программы, выполните следующую команду:

```
integrity_check_tool -v[|--verify] -m[|--manifest] <путь к файлу>
```

где `<путь к файлу>` – это путь к файлу манифеста. По умолчанию утилита использует файл манифеста `integrity_check.xml`, расположенный в директории `/opt/kaspersky/kesl/bin`.

Вы можете запустить утилиту проверки целостности со следующими дополнительными параметрами:

- `-h, --help` – вывод справки о параметрах утилиты.
- `-V, --verbose` – расширенный вывод 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 <файл>`, где `<файл>` – имя файла для вывода событий, произошедших во время проверки. По умолчанию события выводятся в стандартный поток `stdout`.
- `-l, --log-level <0-1000>`, где `<0-1000>` – уровень детализации вывода событий. По умолчанию уровень детализации – 0.

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

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

Управление программой с помощью Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center. Описание приведено для Kaspersky Security Center 11.

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать программу Kaspersky Endpoint Security, настраивать параметры работы программы и запускать задачи на управляемых устройствах.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Перед установкой плагина управления Kaspersky Endpoint Security требуется убедиться, что установлены Kaspersky Security Center и Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable).

В сертифицированной версии программы не поддерживаются следующие функции:

- Управление сетевым экраном;
- Защита от сетевых угроз;
- Контроль устройств;
- механизм автоматической загрузки обновлений программы.

Несмотря на то, что параметры некоторых из этих функций отображаются в плагине управления Kaspersky Endpoint Security в Kaspersky Security Center, невозможно использовать эти функции и настроить их параметры.

Вы можете выполнять следующие действия в Консоли администрирования Kaspersky Security Center:


- просматривать состояние защиты устройств;
- настраивать общие параметры защиты устройств;
- управлять политиками;
- управлять следующими задачами:
 - Антивирусная проверка
 - Добавление ключа
 - Проверка контейнеров
 - Проверка целостности системы по требованию
 - Проверка загрузочных секторов
 - Проверка памяти процессов и памяти ядра
 - Обновление
 - Откат обновлений


В этой главе

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере.....	171
Просмотр состояния защиты компьютера.....	172
Просмотр параметров Kaspersky Endpoint Security.....	173
Управление политиками.....	174
Управление задачами.....	175
Проверка соединения с Сервером администрирования вручную. Утилита klnagchk.....	180
Подключение к Серверу администрирования вручную. Утилита klmover.....	181

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

► Чтобы запустить или остановить Kaspersky Endpoint Security на клиентском компьютере, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите компьютер, на котором вы хотите запустить или остановить программу.
5. Правой клавишей мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.
Откроется окно свойств компьютера.
6. В окне свойств компьютера выберите раздел **Программы**.
Справа в окне свойств компьютера отобразится список программ “Лаборатории Касперского”, установленных на компьютере.
7. Выберите программу Kaspersky Endpoint Security 11.1.0 для Linux.
8. Если вы хотите запустить работу программы, нажмите на кнопку  справа от списка программ “Лаборатории Касперского” или выполните следующие действия:
 - a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 11.1.0 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.
Откроется окно **Параметры Kaspersky Endpoint Security 11.1.0 для Linux** на закладке **Общие**.
 - b. Нажмите на кнопку **Запустить**.

9. Если вы хотите остановить работу программы, нажмите на кнопку  справа от списка программ “Лаборатории Касперского” или выполните следующие действия:

- a. Правой клавишей мыши откройте контекстное меню программы Kaspersky Endpoint Security 11.1.0 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

Откроется окно **Параметры Kaspersky Endpoint Security 11.1.0 для Linux** на закладке **Общие**.

- b. Нажмите на кнопку **Остановить**.

Просмотр состояния защиты компьютера

► Чтобы просмотреть состояние защиты компьютера, выполните следующие действия:

1. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства** выберите закладку **Защита**.

На закладке **Защита** отображается следующая информация о защищаемом компьютере:

- **Статус устройства** – статус клиентского устройства, присвоенный на основе критерия, заданного администратором для статусов антивирусной защиты устройства и активности устройства в сети.
- **Все проблемы** – полный список проблем, обнаруженных управляемыми программами, установленными на клиентских устройствах. Каждая проблема дополняется статусом, который программа предлагает назначить устройству, имеющему эту проблему.
- **Статус постоянной защиты** – статус задачи Защита от файловых угроз, например, *Выполняется* или *Остановлена*. При изменении статуса устройства, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.
- **Последняя проверка по требованию** – дата и время выполнения последней антивирусной проверки на клиентском устройстве.
- **Общее количество обнаруженных угроз** – общее количество угроз, обнаруженных на клиентском устройстве с момента установки антивирусной программы (первой проверки) или с момента последнего сброса счетчика угроз. Чтобы сбросить счетчик, нажмите на кнопку **Обнулить**.
- **Активные угрозы** – количество угроз, которые программе Kaspersky Endpoint Security не удалось вылечить на данный момент.
- **Статус шифрования диска** – текущий статус шифрования файлов на локальных дисках устройства.

Просмотр параметров Kaspersky Endpoint Security

► Чтобы просмотреть параметры Kaspersky Endpoint Security, выполните следующие действия:

1. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
 2. В рабочей области выберите закладку **Устройства**.
 3. Правой клавишей мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
 4. В открывшемся окне **Свойства: <название компьютера>** выберите раздел **Программы**.
 5. В разделе **Программы** в списке установленных программ выберите Kaspersky Endpoint Security 11.1.0 для Linux и в контекстном меню программы выберите пункт **Свойства**.
- В результате откроется окно **Параметры Kaspersky Endpoint Security 11.1.0 для Linux** на разделе **Общие**.

В окне **Параметры Kaspersky Endpoint Security 11.1.0 для Linux** отображается следующая информация о программе Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленной программе:
 - **Номер версии** – номер версии программы Kaspersky Endpoint Security.
 - **Установлено** – дата и время установки программы Kaspersky Endpoint Security на защищаемом компьютере.
 - **Текущее состояние** – состояние задачи Защита от файловых угроз, например: *Выполняется* или *Приостановлена*.
 - **Последнее обновление ПО** – дата и время последнего обновления программных модулей Kaspersky Endpoint Security.
 - **Установленные обновления** – список программных модулей, для которых установлены обновления.
 - **Базы программы** – дата и время последнего обновления антивирусных баз, а также количество записей в базах.
- В разделе **Компоненты** содержится список стандартных задач. Для каждой задачи отображается ее статус (например, *Запущена* или *Остановлена*) и версия.
- В разделе **Ключи** приведена информация об активном и дополнительном ключе:
 - **Тип лицензии** – тип лицензии: коммерческая или пробная.
 - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа.
 - **Дата окончания срока действия лицензии** (поле доступно только для активного ключа) – дата окончания срока действия активного ключа.
 - **Срок действия лицензии** – количество дней, в течение которых действует ключ.
 - **Ограничение** – количество компьютеров, на которых вы можете использовать ключ.
- В разделе **Настройка событий** содержатся события, которые программа Kaspersky Endpoint Security сохраняет в хранилище событий.
- В разделе **Дополнительно** содержится информация о плагине управления программой.

Управление политиками

С помощью политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных компьютеров в группе администрирования при помощи Kaspersky Endpoint Security. Вы можете изменять локально только те параметры, изменение которых не запрещено политикой.

Возможность изменять параметр программы на клиентском компьютере определяется статусом “замка” у параметра в политике:

- Если параметр закрыт “замком” (🔒), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт “замком” (🔓), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

Локальные параметры программы изменяются в соответствии с параметрами политики после первого применения политики.

Вы можете использовать политики для настройки параметров таких задач программы Kaspersky Endpoint Security, как Защита от файловых угроз, Защита от шифрования, Контроль целостности системы при доступе, Управление хранилищем и других (см. раздел “Изменение параметров политики” на стр. [175](#)).

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Удалять политику.
- Изменять состояние политики.

Информацию о работе с политиками, не касающуюся взаимодействия с Kaspersky Endpoint Security, вы можете прочитать в документации для Kaspersky Security Center.

Создание политики

► Чтобы создать политику, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:

- Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать политику для всех управляемых программой Kaspersky Security Center компьютеров.
 - В папке **Управляемые устройства** дерева консоли выберите папку с названием группы администрирования, в состав которой входят интересующие вас компьютеры.
3. В рабочей области выберите закладку **Политики**.
 4. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.
 5. Следуйте указаниям мастера создания политики.

Изменение параметров политики

► Чтобы изменить параметры политики, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** одним из следующих способов:
 - По ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
 - Двойным щелчком мыши.
 - По правой клавише мыши вызовите контекстное меню политики и выберите пункт **Свойства**.

Параметры политики для Kaspersky Endpoint Security включают в себя параметры задач и параметры программы. Раздел **Базовая защита** содержит разделы **Параметры защиты от файловых угроз**, **Области исключений**, **Управление сетевым экраном**, **Защита от веб-угроз** и **Защита от сетевых угроз**. Раздел **Продвинутая защита** содержит разделы **Параметры KSN**, **Параметры защиты от шифрования**, **Параметры контроля целостности системы**, **Контроль устройств** и **Анализ поведения**. Раздел **Общие параметры** содержит разделы **Параметры программы**, **Параметры прокси-сервера**, **Параметры перехватчика**, **Параметры сети**, **Глобальные исключения** и **Хранилища**.

В сертифицированной версии программы некоторые параметры могут быть недоступны для настройки и использования.

5. Измените параметры политики.
6. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Управление задачами

Kaspersky Security Center управляет работой программы Kaspersky Endpoint Security, установленной на компьютерах, с помощью задач (<https://help.kaspersky.com/KSC/11/ru-RU/92435.htm>).

При работе с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

Задачи для наборов компьютеров распространяются только на компьютеры, указанные в параметрах задачи. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Добавление ключа.** В процессе выполнения задачи программа Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Проверка контейнеров.** В процессе выполнения задачи программа Kaspersky Endpoint Security проверяет Docker-контейнеры и образы.
- **Проверка целостности системы по требованию.** В процессе выполнения этой задачи изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- **Проверка загрузочных секторов.** В процессе выполнения задачи программа Kaspersky Endpoint Security проверяет загрузочные сектора компьютера.
- **Проверка памяти процессов и памяти ядра.** В процессе выполнения задачи программа Kaspersky Endpoint Security проверяет системную память компьютера и память ядра.
- **Обновление.** В процессе выполнения задачи программа Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновлений.** В процессе выполнения задачи программа Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Антивирусная проверка.** В процессе выполнения задачи программа Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.

Вы можете выполнять следующие действия над задачами:

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.
Задачу Обновление невозможно приостановить и возобновить. Ее можно только запустить или остановить;
- Создавать новые задачи.
- Изменять параметры задач.

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей программы Kaspersky Endpoint Security перейдите в раздел **Безопасность** (<https://help.kaspersky.com/KSC/11/ru-RU/174017.htm>) окна свойств Сервера администрирования Kaspersky Security Center.

Общая информация о задачах в Kaspersky Security Center приводится в документации для Kaspersky Security Center.

Создание локальной задачи

► Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.
5. Правой клавишей мыши откройте контекстное меню компьютера и выберите пункт **Свойства**.
Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.
7. Нажмите на кнопку **Добавить**, чтобы запустить мастер создания задачи.
8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► Чтобы создать групповую задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

Создание задачи для набора компьютеров

► Чтобы создать задачу для набора компьютеров, выполните следующие действия:



1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** в дереве Консоли администрирования.
3. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите на кнопку **Назначить задачу выборке устройств**.
6. В следующем окне мастера нажмите на кнопку **Обзор**.
Откроется окно **Выборка устройств**.

7. Выберите нужный компьютер и нажмите кнопку **ОК**.
8. Следуйте указаниям мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Если программа Kaspersky Endpoint Security запущена на компьютере (см. раздел “Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере” на стр. 171), вы можете запускать, останавливать, приостанавливать и возобновлять выполнение задач на этом компьютере с помощью Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможно.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить, остановить, приостановить или возобновить выполнение локальной задачи.
5. Выберите пункт **Свойства** в контекстном меню компьютера.
Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.
В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить, остановить, приостановить или возобновить.
8. Выполните одно из следующих действий:
 - Правой клавишей мыши откройте контекстное меню локальной задачи и выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.
 - Нажмите на кнопку  /  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
 - Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства: <Название локальной задачи>**. На закладке **Общие** окна **Свойства: <Название локальной задачи>** нажмите на кнопку **Запустить / Остановить / Приостановить / Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.
В правой части окна отобразится список групповых задач.
4. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить, остановить, приостановить или возобновить.
5. Правой клавишей мыши откройте контекстное меню групповой задачи и выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.

Изменение параметров локальной задачи

► *Чтобы изменить параметры локальной задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры программы.
5. Правой клавишей мыши откройте контекстное меню компьютера и выберите пункт **Свойства**.
Откроется окно свойств компьютера.
6. Выберите раздел **Задачи**.
В правой части окна отобразится список локальных задач.
7. Выберите в списке локальных задач нужную локальную задачу.
8. Выполните одно из следующих действий:
 - Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
 - Нажмите на кнопку **Свойства**.Откроется окно **Свойства: <Название локальной задачи>**.
9. Измените параметры локальной задачи.
10. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров групповой задачи

► *Чтобы изменить параметры групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. В списке групповых задач выберите нужную групповую задачу.
5. Правой клавишей мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Название групповой задачи>**.
6. Измените параметры групповой задачи.
7. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Изменение параметров задачи для набора устройств

► *Чтобы изменить параметры задачи для набора устройств, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Задачи**.
3. В рабочей области в списке задач выберите нужную задачу.
4. По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Название задачи для наборов устройств>**.
5. Измените параметры задачи для набора устройств.
6. В окне **Свойства: <Название задачи для наборов устройств>** нажмите на кнопку **ОК**, чтобы сохранить изменения.

Количество и содержимое разделов зависит от типа выбранной задачи. Содержимое разделов **Общие**, **Уведомления**, **Расписание** и **История ревизий** одинаковое для всех задач. Более подробное описание этих разделов приведено в документации к Kaspersky Security Center.

Проверка соединения с Сервером администрирования вручную. Утилита `klagchk`

В комплект поставки Агента администрирования входит утилита `klagchk`, предназначенная для проверки подключения к Серверу администрирования.

После установки Агента администрирования утилита сохраняется в директории `/opt/kaspersky/klagent/bin` в 32-разрядной операционной системе и в директории `/opt/kaspersky/klagent64/bin` в 64-разрядной операционной системе.

В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- выводит на экран или заносит в файл журнала событий значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;

- записывает в файл журнала событий статистику Агента администрирования (с момента последнего запуска этого компонента) и результаты выполнения утилиты либо выводит информацию на экран;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Синтаксис утилиты

```
klmagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>]  
[-restart]
```

Описание ключей

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу администрирования и результаты работы утилиты в файл журнала. Если этот ключ не используется, параметры, результаты и сообщения об ошибках отображаются на экране.
- `-sp` – показать пароль аутентификации пользователя на прокси-сервере. Этот параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.
- `-savecert <имя файла>` – сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в указанном файле.
- `-restart` – перезапустить Агент администрирования.

Подключение к Серверу администрирования вручную. Утилита klmover

В комплект поставки Агента администрирования входит утилита klmover, предназначенная для управления подключением к Серверу администрирования.

После установки Агента администрирования утилита сохраняется в директории `/opt/kaspersky/klmagent/bin` в 32-разрядной операционной системе и в директории `/opt/kaspersky/klmagent64/bin` в 64-разрядной операционной системе.

В зависимости от используемых ключей Агент выполняет следующие действия при запуске:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис утилиты

```
klmover [-logfile <имя файла>] {-address <адрес сервера>} [-pn <номер  
порта>] [-ps <номер SSL-порта>] [-nossll] [-cert <путь к файлу сертификата>]  
[-silent] [-dupfix]
```

Описание ключей

- `-logfile <имя файла>` – записать результаты работы утилиты в указанный файл. Если этот ключ не используется, результаты и сообщения об ошибках отправляются в `stdout`.
- `-address <адрес сервера>` – адрес Сервера администрирования, используемого для подключения. Это может быть IP-адрес, NetBIOS или DNS-имя компьютера.

- `-pn <номер порта>` – номер порта, по которому устанавливается незашифрованное соединение с Сервером администрирования. По умолчанию используется порт 14000.
- `-ps <номер порта SSL>` – номер SSL-порта, по которому устанавливается зашифрованное соединение с Сервером администрирования по протоколу SSL. По умолчанию используется порт 13000.
- `-nossl` – использовать незашифрованное соединение с Сервером администрирования. Если этот ключ не указан, Агент соединяется с сервером администрирования через зашифрованный протокол SSL.
- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- `-silent` – запустить утилиту в не-интерактивном режиме. Использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – этот файл ключа используется, если способ установки Агента администрирования отличается от способа установки в составе комплекте поставки, например, восстановление с диска.
- `-cloningmode 1` – перейти в режим клонирования.
- `-cloningmode 0` – выйти из режима клонирования.

Использование графического пользовательского интерфейса Kaspersky Endpoint Security

В этом разделе описана работа в программе Kaspersky Endpoint Security с использованием графического пользовательского интерфейса.

В этой главе

Локальное включение и выключение графического пользовательского интерфейса	183
Интерфейс программы	184
Управление задачами и компонентами	185
Отчеты	188
Просмотр объектов в хранилище	190
Создание файла трассировки	190

Локальное включение и выключение графического пользовательского интерфейса

Вы можете включить или выключить графический пользовательский интерфейс Kaspersky Endpoint Security локально с помощью командной строки.

Для включения и выключения графического пользовательского интерфейса требуются root-права. Если графический пользовательский интерфейс выключен, пользователи, не обладающие root-правами, не смогут запустить графический пользовательский интерфейс на своих локальных компьютерах.

► Чтобы включить или выключить графический пользовательский интерфейс, выполните следующие действия:

1. Запустите конфигурационный скрипт программы:

```
/opt/kaspersky/kesl/bin/kesl-setup.pl -G
```

Отображается запрос.

2. Выполните одно из следующих действий:

- Если вы хотите включить графический пользовательский интерфейс, нажмите **Y**, а затем, при необходимости, укажите пользователя, которому требуется назначить роль администратора.

Если вы включите графический пользовательский интерфейс, пользователи без root-прав смогут запускать до пяти задачи антивирусной проверки одновременно.

Если пользователь вошел в систему, для него запускается графический пользовательский интерфейс, если доступны все необходимые библиотеки. В области уведомлений панели задач появится значок программы и создается ярлык.

- Если вы хотите выключить графический пользовательский интерфейс, введите N.

Программа запрещает пользователям запускать графический пользовательский интерфейс локально. Значок программы и ярлык удаляются.

Интерфейс программы

Этот раздел содержит информацию об основных элементах графического пользовательского интерфейса программы.

Значок программы в области уведомлений

После включения графического пользовательского интерфейса Kaspersky Endpoint Security значок программы появляется справа в области уведомлений панели задач. Значок обеспечивает доступ к контекстному меню и главному окну программы. Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security 11.1.0 для Linux.** Открывает главное окно программы. В главном окне программы отображается состояние защиты вашего компьютера, а также состояние задач антивирусной проверки и обновлений. Вы также можете перейти в окно **Отчеты**, **Хранилище**, **Параметры** или **Поддержка**.
- **Выход.** Выход из графического пользовательского интерфейса Kaspersky Endpoint Security.

Вы можете открыть контекстное меню значка программы, щелкнув правой кнопкой мыши по значку программы в области уведомлений.

Главное окно программы

В главном окне Kaspersky Endpoint Security находятся элементы интерфейса, предоставляющие доступ к функциям программы.

Главное окно программы разделено на несколько частей:

- В центральной части окна отображается статус защиты вашего компьютера. При щелчке мышью в этой части окна откроется окно **Центр защиты**.
- На закладке **Проверка** отображается состояние задачи антивирусной проверки и количество обнаруженных угроз. По щелчку по этой закладке открывается окно **Проверка**. В этом окне вы можете запустить и остановить задачи антивирусной проверки, задачу проверки памяти процессов и памяти ядра и задачу проверки загрузочных секторов. Вы также можете просмотреть отчеты для этих задач.
- На закладке **Обновление** отображается состояние задачи Обновление и состояние антивирусных баз. По щелчку по этой закладке открывается окно **Обновление**. В этом окне вы можете запустить или остановить задачи обновления, а также просмотреть отчеты для этих задач.
- В нижней части главного окна программы находятся следующие элементы:
 - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором можно просмотреть статистику задач и различные отчеты.

- Кнопка **Хранилище**. При нажатии на эту кнопку открывается окно **Хранилище**, в котором содержится информация об объектах в хранилище.
- Кнопка **Параметры**. При нажатии на эту кнопку открывается окно **Параметры**, в котором можно включить или отключить участие в Kaspersky Security Network, а также задачи Защита от файловых угроз, Контроль целостности системы, Управление сетевым экраном, Защита от шифрования, Защита от веб-угроз, Контроль устройств, Проверка съемных дисков, Защита от сетевых угроз и Анализ поведения.
- Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором содержится информация о текущей версии Kaspersky Endpoint Security, лицензии, статусе ключа, статусе баз, операционной системе, а также ссылки на информационные ресурсы “Лаборатории Касперского”.

Вы можете открыть главное окно программы Kaspersky Endpoint Security одним из следующих способов:

- Двойным щелчком мыши или щелчком правой клавиши мыши по значку программы в области уведомлений панели задач.
- Щелчком правой клавиши мыши по названию программы откройте контекстное меню и выберите **Kaspersky Endpoint Security 11.1.0 для Linux**.

Управление задачами и компонентами

По умолчанию графический пользовательский интерфейс программы Kaspersky Endpoint Security позволяет запускать и останавливать следующие задачи:

- Задача полной проверки (Scan_My_Computer) (см. раздел “Задача антивирусной проверки (Scan_My_Computer ID:2)” на стр. [89](#)).
- Задачи антивирусной проверки (Scan_File, Boot_Scan, Memory_Scan) (см. раздел “Запуск и остановка задач проверки” на стр. [186](#)).
- Задачи обновления (Обновление, Откат обновлений) (см. раздел “Запуск и остановка задач обновления” на стр. [186](#)).

Графический пользовательский интерфейс программы Kaspersky Endpoint Security также позволяет включать и выключать следующие компоненты:

- Защита от файловых угроз (см. раздел “Задача Защита от файловых угроз (File_Threat_Protection ID:1)” на стр. [79](#)).
- Контроль целостности системы (см. раздел “Задача Контроль целостности системы (Integrity_Monitoring ID:11)” на стр. [122](#)).
- Защита от шифрования (см. раздел “Задача Защита от шифрования (AntiCryptor ID:13)” на стр. [130](#)).
- Защита от веб-угроз (см. раздел “Задача Защита от веб-угроз (File_Threat_Protection ID:14)” на стр. [136](#)).
- Проверка съемных дисков (см. раздел “Задача Проверка съемных дисков (Removable_Drives_Scan ID: 16)” на стр. [139](#)).
- Анализ поведения (см. раздел “Задача Анализ поведения (Behavior_Detection ID: 20)” на стр. [158](#)).
- Защита от сетевых угроз.
- Управление сетевым экраном.
- Контроль устройств.

Кроме того, вы можете управлять своим участием в Kaspersky Security Network (см. раздел “Управление участием в Kaspersky Security Network” на стр. [187](#)).

Запуск и остановка задач проверки

С помощью графического пользовательского интерфейса программы Kaspersky Endpoint Security вы можете запускать и останавливать задачи полной проверки, задачи антивирусной проверки, задачи проверки памяти процессов и памяти ядра и задачи проверки загрузочных секторов.

► *Чтобы запустить или остановить задачу проверки, выполните следующие действия:*

1. Откройте главное окно программы (см. стр. [184](#)).
2. По кнопке **Проверка**, расположенной в главном окне программы, откройте окно **Проверка**.
3. Выполните одно из следующих действий:
 - Если вы хотите запустить задачу, нажмите на кнопку **Запустить** под той задачей, которую вы хотите запустить.
Отобразится ход выполнения задачи.
 - Если вы хотите остановить задачу, нажмите на кнопку **Остановить** под той задачей проверки, которую вы хотите остановить.
Задача проверки останавливается, и отображается информация о проверенных объектах и обнаруженных угрозах.
4. При необходимости вы можете нажать на кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком программы в правой части панели задач.

Запуск и остановка задач обновления

С помощью графического пользовательского интерфейса программы Kaspersky Endpoint Security вы можете запускать и останавливать задачи **Обновление** и **Откат обновления баз**.

► *Чтобы запустить или остановить задачу обновления, выполните следующие действия:*

1. Откройте главное окно программы (см. стр. [184](#)).
2. По кнопке **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. Выполните одно из следующих действий:
 - Если вы хотите запустить задачу, нажмите на кнопку **Запустить** под той задачей, которую вы хотите запустить.
Отобразится ход выполнения задачи.
При успешном завершении задачи обновления становится доступна ссылка **Откат обновления**, с помощью которой вы можете откатить последнее обновление.
 - Если вы хотите остановить задачу, нажмите на кнопку **Остановить** под той задачей, которую вы хотите остановить.
Задача будет остановлена.
4. При необходимости вы можете нажать на кнопку **Показать отчет**, чтобы просмотреть отчет по задаче.

► Чтобы запустить задачу отката обновления, выполните следующие действия:

1. Откройте главное окно программы (см. стр. [184](#)).
2. По кнопке **Обновить**, расположенной в главном окне программы, откройте окно **Обновление**.
3. В разделе **Обновление** перейдите по ссылке **Откат обновления**, чтобы откатить последнее успешное обновление баз.

Включение и выключение компонентов программы

С помощью графического пользовательского интерфейса программы Kaspersky Endpoint Security вы можете в любой момент включить или выключить следующие компоненты программы: Защита от файловых угроз, Управление сетевым экраном, Защита от шифрования и Контроль целостности системы.

Если компонент включен, доступна кнопка **Отключить**. По умолчанию включен только компонент Защита от файловых угроз.

Если компонент выключен, доступна кнопка **Включить**.

► Чтобы включить или выключить компонент, выполните следующие действия:

1. Откройте главное окно программы (см. стр. [184](#)).
2. В нижней части главного окна программы нажмите на кнопку **Параметры**.
Откроется окно **Параметры**.
3. В окне **Параметры** выполните следующие действия для нужного компонента:
 - Чтобы включить компонент, нажмите на кнопку **Включить**.
 - Чтобы отключить компонент, нажмите на кнопку **Отключить**.

Управление участием в Kaspersky Security Network

Вы можете управлять своим участием в Kaspersky Security Network в любой момент.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

► Чтобы включить Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы (см. стр. [184](#)).
2. В нижней части главного окна программы нажмите на кнопку **Параметры**.
Откроется окно **Параметры**.
3. В окне **Параметры** выберите один из следующих вариантов:
 - **Kaspersky Security Network со статистикой**, чтобы включить Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.

- **Kaspersky Security Network без статистики**, чтобы получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках угроз.
4. Нажмите на кнопку **Включить**.
 5. В окне **Участие в Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите один из следующих вариантов:
 - **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Положения о KSN** – чтобы включить Kaspersky Security Network.
 - **Я не принимаю положения и условия настоящего Положения о KSN** – чтобы отказаться от использования Kaspersky Security Network.
 6. Нажмите **ОК**.
Кнопка **ОК** недоступна, если выбран вариант **Не выбрано**.

► *Чтобы выключить Kaspersky Security Network, выполните следующие действия:*

1. Откройте главное окно программы (см. стр. [184](#)).
2. В нижней части главного окна программы нажмите на кнопку **Параметры**.
Откроется окно **Параметры**.
3. В окне **Параметры** нажмите на кнопку **Отключить**.
4. В открывшемся окне выполните одно из следующих действий:
 - Нажмите на кнопку **Да**, чтобы подтвердить отключение Kaspersky Security Network.
 - Нажмите **Отмена**, чтобы продолжать участвовать в Kaspersky Security Network.

Отчеты

В этом разделе содержится информация о том, как просматривать отчеты в графическом пользовательском интерфейсе программы Kaspersky Endpoint Security.

В этом разделе

Принципы работы с отчетами.....	188
Просмотр отчетов	189

Принципы работы с отчетами

Информация о работе задач Kaspersky Endpoint Security регистрируется в отчетах. Данные в отчетах представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события расположены в графах таблицы. События, зарегистрированные в работе разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты, перечисленные в меню слева:

- **Статистика**. Содержит статистические данные о задаче Защита от файловых угроз и задачах антивирусной проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.

При остановке задачи Защита от файловых угроз происходит сброс статистики. Сброса статистики для задач антивирусной проверки не происходит. Вместо этого статистика накапливается за время, пока программа установлена на компьютере.

- **Системный аудит.** Этот отчет содержит информацию о событиях, которые произошли во время взаимодействия пользователя с программой. Он также содержит информацию о событиях, которые произошли во время обычной работы программы.
- **Защита от угроз.** Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих компонентов Kaspersky Endpoint Security:
 - Защита от шифрования
 - Контроль целостности системы
 - Управление сетевым экраном
 - Защита от веб-угроз
 - Контроль устройств
 - Проверка съемных дисков
 - Защита от сетевых угроз
 - Анализ поведения
 - Защита от файловых угроз
- **Задачи по требованию.** Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы следующих задач Kaspersky Endpoint Security:
 - Задачи проверки
 - Обновление
 - Проверка целостности

В отчетах применяются следующие уровни важности событий:

- **Информационные события.** События справочного характера, как правило, не содержащие важной информации.
- **Важные события.** События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- **Критические события.** События критической важности, указывающие на проблемы в работе программы Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменить представление данных на экране следующими способами:

- отфильтровать список событий по времени;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке.

Просмотр отчетов

► *Чтобы просмотреть отчеты, выполните следующие действия:*

1. Откройте главное окно программы.

2. В нижней части главного окна программы нажмите на кнопку **Отчеты**.

Откроется окно **Отчеты**.

3. Чтобы просмотреть конкретный отчет, в левой части окна **Отчеты** выберите нужную задачу из списка задач.

В правой части окна отобразится отчет, содержащий список событий о работе выбранной задачи Kaspersky Endpoint Security.

По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата**. Вы можете выбрать другой порядок, щелкнув по заголовку нужной графы.

4. Чтобы просмотреть в отчете подробную сводную информацию о каждом событии, выберите соответствующее событие в отчете.

Сводная информация о событии отображается в нижней части окна.

Просмотр объектов в хранилище

► *Чтобы просмотреть объекты, которые программа Kaspersky Endpoint Security переместила в хранилище, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Хранилище**.

В открывшемся окне отображается информация об объектах в хранилище.

Вы можете просмотреть следующую информацию об объектах в хранилище:

- название угрозы;
- полный путь к объекту;
- дата перемещения объекта в хранилище;
- дата удаления объекта из хранилища (это поле отображается, если указан параметр `DaysToLive`);
- размер объекта.

Вы можете восстановить объекты из хранилища в их исходные директории. Вы также можете удалить объекты из хранилища. Удаленные объекты восстановить невозможно. Информация об этих действиях записывается в журнал событий.

Создание файла трассировки

► *Чтобы создать файл трассировки, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Поддержка**.
3. В окне **Поддержка** нажмите на кнопку **Трассировка**.
4. В раскрывающемся списке **Уровень** выберите уровень трассировки.

Рекомендуется уточнить необходимый уровень трассировки у специалиста из Службы технической поддержки “Лаборатории Касперского”. По умолчанию для уровня трассировки установлено значение **Диагностический (300)**.

5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.
6. Чтобы остановить процесс трассировки, нажмите на кнопку **Отключить**.

Созданные файлы трассировки хранятся в директории `/var/log/kaspersky/kesl/`. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные (см. раздел “Содержимое файлов трассировки и их хранение” на стр. [195](#)).

Устранение уязвимостей и установка критических обновлений в программе

“Лаборатория Касперского” может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления).

Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений “Лаборатории Касперского”. Уведомления о выпуске критических обновлений публикуются на веб-сайте <http://support.kaspersky.ru/general/certificates> и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу требуется периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта “Лаборатории Касперского” (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки “Лаборатории Касперского” (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме “Лаборатории Касперского” (<http://forum.kaspersky.com>).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел “Способы получения технической поддержки” на стр. [130](#)).

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этой главе

Способы получения технической поддержки	194
Техническая поддержка по телефону	194
Техническая поддержка через Kaspersky CompanyAccount	195
Содержимое файлов трассировки и их хранение	195
Содержимой файлов дампа и их хранение	196

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 “Лаборатории Касперского”. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос с портала My Kaspersky. Этот метод позволяет вам связаться с нашими специалистами с помощью формы запроса.

Техническая поддержка доступна только пользователям, которые приобрели лицензию на использование программы. Техническая поддержка не предоставляется пользователям, использующим пробные версии.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки Лаборатории Касперского. 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>).

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. Вы можете использовать Kaspersky CompanyAccount для отслеживания статуса ваших онлайн-запросов и хранения их истории.

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.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Содержимое файлов трассировки и их хранение

Пользователи лично отвечают за безопасность данных, хранящихся на их компьютерах, в частности, за контроль и ограничение доступа к данным до момента их передачи в “Лабораторию Касперского”.

Файлы трассировки хранятся на компьютере в течение всего времени использования программы и удаляются без возможности восстановления при удалении программы.

По умолчанию файлы трассировки хранятся в директории `/var/log/kaspersky/kesl/`. Вы можете просматривать данные, хранящиеся в файлах трассировки. Для доступа к заданной по умолчанию директории хранения файлов трассировки требуются root-права.

Во всех файлах трассировки хранятся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент программы, инициировавший событие;

- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом программы, и результат выполнения этой команды.

Программа Kaspersky Endpoint Security сохраняет пароли пользователей в файл трассировки только в зашифрованном виде.

Кроме общих данных в файлах трассировки могут храниться следующие данные:

- статусы компонентов Kaspersky Endpoint Security и их рабочие данные;
- данные о действиях пользователей в программе;
- данные об оборудовании, установленном на компьютере;
- данные обо всех объектах и событиях операционной системы, включая данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов “Лаборатории Касперского” (например, версия антивирусных баз).

Содержимое файлов дампа и их хранение

Файлы дампа могут содержать персональные данные. Чтобы обеспечить контроль и ограничение доступа к данным, требуется самостоятельно позаботиться о безопасности файлов дампа.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания файла дампа. Файл дампа может также содержать персональные данные.

Файлы дампа формируются автоматически при сбое программы и хранятся на компьютере в течение всего времени использования программы. Файлы дампа удаляются без возможности восстановления при удалении программы.

Файлы дампа хранятся в следующих директориях:

- `/var/opt/kaspersky/kesl/common/dumps`
- `/var/opt/kaspersky/kesl/common/dumps-user`

Для доступа к файлам дампа требуются root-права.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 5. 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 пользователь

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этой главе

Конфигурационные файлы задачи по умолчанию	198
Коды возврата командной строки.....	204
Значения параметров программы в сертифицированном состоянии	204

Конфигурационные файлы задачи по умолчанию

Этот раздел содержит информацию о конфигурационных файлах по умолчанию для задач Kaspersky Endpoint Security.

Конфигурационные файлы можно изменить в любой момент. Вы также можете изменить значения параметров из командной строки.

Правила редактирования конфигурационных файлов Kaspersky Endpoint Security

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле требуется указать все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, помещайте его только в этой секции. В пределах одной секции вы можете помещать параметры в любом порядке.
- Закрывайте имена секций в квадратные скобки [].
- Вводите значения параметров в формате имя параметра=значение (пробелы между именем параметра и его значением не обрабатываются).

Пример:

```
[ScanScope.item_0000]  
AreaDesc=Home  
AreaMask.item_0000=*doc  
Path=/home
```

Символы “пробел” и “табуляция” игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.

- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

Пример:

```
AreaMask.item_0000=*xml
```

```
AreaMask.item_0001=*doc
```

- Соблюдайте регистр при вводе значений параметров следующих типов:
 - имена (маски) проверяемых объектов и объектов исключения;
 - названия (маски) угроз;

При вводе остальных значений параметров соблюдать регистр не требуется.

- Указывайте значения параметров булевского типа следующим образом: Yes - No.
- Закрывайте в кавычки строковые значения, содержащие символ “пробел” (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате “ГГГГ-ММ-ДД ЧЧ:ММ:СС”).
Остальные значения вы можете вводить как в кавычках, так и без них.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

Одиночная кавычка в начале или в конце строки считается ошибкой.

Конфигурационный файл задачи Защита от файловых угроз

```
ScanArchived=No
```

```
ScanSfxArchived=No
```

```
ScanMailBases=No
```

```
ScanPlainMail=No
```

```
TimeLimit=60
```

```
SizeLimit=0
```

```
FirstAction=Recommended
```

```
SecondAction=Block
```

```
UseExcludeMasks=No
```

```
UseExcludeThreats=No
```

```
ReportCleanObjects=No
```

```
ReportPackedObjects=No
```

```
ReportUnprocessedObjects=No
```

```
UseAnalyzer=Yes
```

```
HeuristicLevel=Recommended
```

```
UseIChecker=Yes
ScanByAccessType=SmartCheck
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Антивирусная проверка

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
ScanPriority=Idle
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```


Конфигурационный файл задачи Выборочная проверка

```
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
ScanPriority=Normal
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Конфигурационный файл задачи Проверка загрузочных секторов

```
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
Action=Disinfect
DeviceNameMasks.item_0000=/**
```

Конфигурационный файл задачи Проверка памяти процессов и памяти ядра

```
UseExcludeThreats=No  
ReportCleanObjects=No  
ReportUnprocessedObjects=No  
Action=Disinfect
```

Конфигурационный файл задачи Обновление

```
SourceType="KLServers"  
UseKLServersWhenUnavailable=Yes  
IgnoreProxySettingsForKLServers=No  
IgnoreProxySettingsForCustomSources=No  
ApplicationUpdateMode=Disabled  
ConnectionTimeout=10
```

Конфигурационный файл задачи Управление хранилищем

```
DaysToLive=90  
BackupSizeLimit=0  
BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Конфигурационный файл задачи Контроль целостности системы

```
UseExcludeMasks=No  
[ScanScope.item_0000]  
AreaDesc=Kaspersky internal objects  
UseScanArea=Yes  
Path=/opt/kaspersky/kesl/  
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от шифрования

```
UseHostBlocker=Yes  
BlockTime=30  
UseExcludeMasks=No  
[ScanScope.item_0000]  
AreaDesc=Все общие папки  
UseScanArea=Yes
```

```
Path=AllShared  
AreaMask.item_0000=*
```

Конфигурационный файл задачи Защита от веб-угроз

```
UseTrustedAddresses=Yes  
ActionOnDetect=Block  
CheckMalicious=Yes  
CheckPhishing=Yes  
UseHeuristicForPhishing=Yes  
CheckAdware=No  
CheckOther=No
```

Конфигурационный файл задачи Проверка съемных дисков

```
ScanRemovableDrives=NoScan  
ScanOpticalDrives=NoScan  
BlockDuringScan=No
```

Конфигурационный файл задачи Проверка контейнеров

```
ScanArchived=Yes  
ScanSfxArchived=Yes  
ScanMailBases=No  
ScanPlainMail=No  
TimeLimit=120  
SizeLimit=0  
FirstAction=Recommended  
SecondAction=Skip  
UseExcludeMasks=No  
UseExcludeThreats=No  
ReportCleanObjects=No  
ReportPackedObjects=No  
ReportUnprocessedObjects=No  
UseAnalyzer=Yes  
HeuristicLevel=Recommended  
UseIChecker=Yes
```

```
ScanContainers=Yes
ContainerNameMask=*
ScanImages=Yes
ImageNameMask=*
DeepScan=No
ScanPriority=Idle
ContainerScanAction=StopContainerIfFailed
ImageAction=Skip
```

Вы можете использовать этот же конфигурационный файл для задачи Выборочная проверка контейнеров (см. раздел “Задача Выборочная проверка контейнеров (Container_Scan ID: 19)” на стр. [150](#)).

Коды возврата командной строки

В программе предусмотрены следующие коды возврата командной строки:

- 0 – команда / задача выполнена успешно;
- 1 – общая ошибка в аргументах команды;
- 2 – ошибка в переданных настройках программы;
- 64 – программа Kaspersky Endpoint Security не запущена;
- 66 – антивирусные базы не загружены (используется только командой `kesl-control --app-info`);
- 67 – активация 2.0 завершилась с ошибкой из-за сетевых проблем;
- 68 – выполнение команды невозможно, так как программа работает под политикой;
- 128 – неизвестная ошибка;
- 65 – все остальные ошибки.

Значения параметров программы в сертифицированном состоянии

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.

Таблица 6. Параметры и их значения для программы в сертифицированном состоянии

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
<code>FirstAction</code>	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки контейнеров	Одно из следующих значений: <ul style="list-style-type: none"> <code>Disinfect</code> – программа пытается вылечить объект, сохранив копию объекта в Хранилище. Если лечение невозможно, программа оставляет объект неизменным. <code>Remove</code> – программа удаляет зараженный объект, предварительно создав его резервную копию. <code>Recommended</code> – программа автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе.
<code>SecondAction</code>	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки контейнеров	Если значение <code>FirstAction=Disinfect</code> : <code>Remove</code> – программа удаляет зараженный объект, предварительно создав его резервную копию.
<code>Action</code>	Задача проверки памяти процессов и памяти ядра, задача проверки загрузочных секторов	<code>Disinfect</code> – программа пытается вылечить объект, сохранив копию объекта в Хранилище.
<code>UseAnalyzer</code>	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки загрузочных секторов, задача проверки контейнеров	<code>Yes</code> – эвристический анализатор включен.
<code>HeuristicLevel</code>	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки загрузочных секторов, задача проверки контейнеров	Одно из следующих значений: <ul style="list-style-type: none"> <code>Light</code> – наименее тщательная проверка, минимальная загрузка системы; <code>Medium</code> – средний уровень эвристического анализа, сбалансированная загрузка системы; <code>Deep</code> – наиболее тщательная проверка, максимальная загрузка системы; <code>Recommended</code> – рекомендуемое значение.

Название параметра	Сущность, к которой относится параметр	Значение параметра в сертифицированном состоянии программы
ScanArchived	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки контейнеров	Yes – проверять архивы.
ScanSfxArchived	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки контейнеров	Yes – проверять самораспаковывающиеся архивы.
ScanMailBases	Задача Защита от файловых угроз, задача антивирусной проверки, задача выборочной проверки, задача проверки контейнеров	Yes – проверять файлы почтовых баз.
ScanByAccessType	Задача Защита от файловых угроз	Open – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
SourceType	Задача обновления	Одно из следующих значений: <ul style="list-style-type: none"> • <code>KLServers</code> – программа получает обновления с одного из серверов обновлений “Лаборатории Касперского”. • <code>SCServer</code> – программа загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. • <code>Custom</code> – программа загружает обновления из пользовательского источника (локальной или сетевой директории (SMB / NFS), смонтированной пользователем, или FTP-, HTTP- или HTTPS-сервера).
ApplicationUpdateMode	Задача обновления	Disabled – не загружать и не устанавливать обновления программы.
UseKSN	Общие параметры программы	No – выключить использование Kaspersky Security Network.

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в директории установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Amazon – товарный знак или зарегистрированные в США и / или других странах товарный знак, принадлежащий Amazon.com, Inc. или аффилированным компаниям.

Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Outlook и Visual C++ – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat Enterprise Linux – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.