KASPERSKY lab

Kaspersky Security Center

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.0.0.1131

Обозначение документа: 643.46856491.00069-06 90 01

Содержание

О Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Программа Kaspersky Security Center адресована администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях.

При помощи Kaspersky Security Center вы можете:

- Формировать иерархию Серверов администрирования для управления сетью собственной организации, а также сетями удаленных офисов или организаций-клиентов.

  Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает поставщик услуг.

- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Управлять системой антивирусной безопасности, построенной на основе программ "Лаборатории Касперского".
- Централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ "Лаборатории Касперского" и других производителей программного обеспечения.
- Удаленно управлять программами "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.
- Централизованно распространять ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе программ и устройств.
- Получать уведомления о критических событиях в работе программ "Лаборатории Касперского".
- Управлять мобильными устройствами.
- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.
- Проводить инвентаризацию оборудования, подключенного к сети организации.
- Централизованно работать с файлами, помещенными программами безопасности на карантин или в резервное хранилище, а также с файлами, обработка которых отложена программами безопасности.

В этом разделе

Об этом документе

Настоящий документ представляет собой руководство по эксплуатации программного изделия "Kaspersky Security Center 11" (далее также "Kaspersky Security Center", "программа").

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 эксплуатация и администрирование Kaspersky Security Center, а также поддержка организаций, использующих Kaspersky Security Center.

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center вы можете получить общую информацию о программе, ее возможностях и особенностях работы (https://www.kaspersky.ru/small-to-medium-business-security/security-center).

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Security Center в Базе знаний (https://support.kaspersky.ru/ksc11), вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Security Center и с другими программами "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

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

Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 939).

О программе

Программа Kaspersky Security Center (далее также "программа"), представляющее собой средство антивирусной защиты типа "А" второго класса защиты, предназначенное для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации, в том числе в изолированном периметре. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

В программе реализованы следующие функции безопасности:

- аудит безопасности программы;
- управление безопасностью;
- сигнализация;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных программ (вирусов) (БД ПКВ);
- централизованная установка компонентов САВЗ;
- поиск уязвимостей на управляемых АРМ.

Комплект поставки

Вы можете приобрести программу через интернет-магазины "Лаборатории Касперского" (например, на сайте http://www.kaspersky.ru) или компаний-партнеров.

Приобретая Kaspersky Security Center через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

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

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с 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 попыток 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.

Аппаратные и программные требования

Сервер администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Программные требования:

- Microsoft® Data Access Components (MDAC) 2.8;
- Microsoft Windows® DAC 6.0;
- Microsoft Windows Installer 4.5.

Операционная система:

- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций (New in RS3) (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;
- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;
- Windows Small Business Server 2008 Standard / Premium 64-разрядная;
- Windows Server® 2019 64-разрядная;
- Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
- Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;
- Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709)) (LTSB/CBB) 64-разрядная;
- Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
- Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;

- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2008 R2 Standard Service Pack 1 64-разрядная;
- Windows Server 2008 with Service Pack 2 (все редакции);
- Microsoft Windows Server 2008 Foundation Service Pack 2 32-разрядная / 64-разрядная;
- Microsoft Windows Storage Server 2016 64-разрядная;
- Microsoft Windows Storage Server 2012 R2 64-разрядная;
- Microsoft Windows Storage Server 2012 64-разрядная;
- Microsoft Windows Storage Server 2008 R2 64-разрядная;

Сервер баз данных (может быть установлен на другой машине):

- Microsoft SQL Server® 2008 Express 32-разрядная;
- Microsoft SQL Server 2008 R2 Express 64-разрядная;
- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 на Windows 64-разрядная;
- MySQL Standard Edition 5.6 32-разрядная / 64-разрядная;
- MySQL Enterprise Edition 5.6 32-разрядная / 64-разрядная;
- MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon™ RDS и Microsoft

Azure™.

Поддерживаются следующие платформы виртуализации:

- VMware™ vSphere™ 6;
- VMware vSphere 6.5.
- VMware Workstation 14 Pro;
- Microsoft Hyper-V® Server 2008 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 1 64-разрядная;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Citrix® XenServer® 7;
- Citrix XenServer 7.1 LTSR.
- Parallels Desktop® 11;
- Oracle® VM VirtualBox 5.x.

Сервер мобильных устройств iOS™ Mobile Device Management (iOS MDM)

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

Сервер мобильных устройств Exchange ActiveSync

Программные и аппаратные требования для Сервера мобильных устройств Exchange ActiveSync полностью включены в требования для сервера Microsoft Exchange Server.

Поддерживается работа с Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 и Microsoft Exchange Server 2013.

Консоль администрирования

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.

- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования);
- Microsoft Management Console 2.0;
- Microsoft Windows Installer 4.5;
- Microsoft Internet Explorer® 9.0 и выше при работе с Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 или Microsoft Windows Vista®;
- Microsoft Internet Explorer 10.0 и выше при работе с Microsoft Windows 8 и 10;
- Microsoft Edge при работе с Microsoft Windows 10.

Агент администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Microsoft Windows Embedded POSReady 2009 32-разрядная;
- Microsoft Windows Embedded POSReady 7 32-разрядная / 64-разрядная;
- Microsoft Windows Embedded Standard 7 Service Pack 1 32-разрядная / 64-разрядная;
- Microsoft Windows Embedded 8 Standard 32-разрядная / 64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Update 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Home RS1 (Anniversary Update, v1607) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS1 (Anniversary Update, v1607) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, v1607) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS1 (Anniversary Update, v1607) 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Home RS2 (Creators Update, v1703) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS2 (Creators Update, v1703) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS2 (Creators Update, v1703) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS2 (Creators Update, v1703) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Home RS5 (октябрь 2018) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS5 (октябрь 2018) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (октябрь 2018) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS5 (октябрь 2018) 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная;
- Microsoft Windows XP Professional for Embedded Systems 32-разрядная;
- Microsoft Essential Business Server 2008 Standard / Premium 64-разрядная;
- Windows Small Business Server 2008 Standard / Premium 64-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;
- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Home Server 2011 64-разрядная;
- Microsoft Windows MultiPoint™ Server 2011 Standard / Premium 64-разрядная;
- Microsoft Windows Server 2008 Foundation Service Pack 2 32-разрядная / 64-разрядная;

- Microsoft Windows Server 2008 Service Pack 2 (все редакции) 32-разрядная / 64-разрядная;
- Windows Server 2008 R2 Standard Service Pack 1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
- Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;
- Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
- Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709)) (LTSB/CBB) 64-разрядная;
- Windows Server 2019 64-разрядная;
- Microsoft Windows Storage Server 2008 R2 64-разрядная;
- Microsoft Windows Storage Server 2016 64-разрядная;
- Microsoft Windows Storage Server 2012 64-разрядная;
- Microsoft Windows Storage Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2008 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 1 64-разрядная;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная.

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно (см. раздел "Развертывание Агента администрирования и программы безопасности" на стр. 108).
Вы можете получить сведения о последней версии аппаратных и программных требований на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе Системные требования.
Агент администрирования для Linux и Агент администрирования для macOS предоставляются вместе с программами безопасности "Лаборатории Касперского" для этих операционных систем.

См. также:

Список поддерживаемых программ "Лаборатории Касперского"

Kaspersky Security Center поддерживает удаленную установку и управление следующими программами "Лаборатории Касперского":

- **Для рабочих станций:**
  - Kaspersky Endpoint Security 10 для Windows (для рабочих станций): 10 Service Pack 1 Maintenance Release 3 (*10.2.5.3201*), 10 Service Pack 1 Maintenance Release 4 (*10.2.6.3733*), 10 Service Pack 2 (*10.3.0.6294*), 10 Service Pack 2 Maintenance Release 1 (*10.3.0.6294 mr1*), 10 Service Pack 2 Maintenance Release 2 (*10.3.0.6294 mr2*), 10 Service Pack 2 Maintenance Release 3 (*10.3.3.275*);
  - Kaspersky Endpoint Security 11 для Windows;
  - Kaspersky Endpoint Security 11.1 для Windows;
  - Kaspersky Endpoint Security 10 для Linux: 10 Service Pack 1 (*10.1*), 10 Service Pack 1 Maintenance Release 1;
  - Kaspersky Endpoint Security 10 для Mac: 10 Service Pack 1 (*10.1.0.622*), 10 Service Pack 2 (*10.2.0.267*), 10 Service Pack 2 Maintenance Release 1 (*10.2.1.319*);
  - Kaspersky Endpoint Security 11 для Mac;
  - Kaspersky Embedded Systems Security for Windows: 1.1 (*1.1.0.104*), 1.1MR1 (*1.2.0.300*), 2.0 (*2.0.0.385*), 2.2.

- **Kaspersky Industrial Cybersecurity**
  - Kaspersky Industrial Cybersecurity for Nodes: 1.0, 2.1, 2.2;
  - Kaspersky Industrial Cybersecurity for Networks: 1.0, 1.4, 2.0 (*2.0.0.113*), 2.5 (*2.5.0.309*), 2.6.
- **Для мобильных устройств:**
  - Kaspersky Security 10 для мобильных устройств (Kaspersky Endpoint Security для Android™): Service Pack 1 Maintenance Release 3 (*10.5.113.0*), Service Pack 2 (*10.6.0.0*), Service Pack 2 Maintenance Release 1 (*10.6.1.0*), Service Pack 2 Maintenance Release 1 U1 (*10.6.1.1*), Service Pack 2 Maintenance Release 2 (*10.6.2.1110*), Service Pack 3 (*10.7.0.97*), Service Pack 3 U2 (*10.7.0.106*), Service Pack 3 Maintenance Release 1 (*10.7.1.47*), Service Pack 4;
  - Kaspersky Device Management для iOS.
- **Для файловых серверов:**
  - Kaspersky Endpoint Security 10 для Windows (для файловых серверов): 0 Service Pack 1 Maintenance Release 3 (*10.2.5.3201*), 10 Service Pack 1 Maintenance Release 4 (*10.2.6.3733*), 10 Service Pack 2 (*10.3.0.6294*), 10 Service Pack 2 Maintenance Release 1 (*10.3.0.6294 mr1*), 10 Service Pack 2 Maintenance Release 2 (*10.3.0.6294 mr2*), 10 Service Pack 2 Maintenance Release 3 (*10.3.3.275*);
  - Kaspersky Endpoint Security 11 для Windows (для файловых серверов);
  - Kaspersky Endpoint Security 11.1 для Windows (для файловых серверов);
  - Антивирус Касперского 8.0 для Linux File Server (*8.0.4.312*);
  - Kaspersky Security 10 для Windows Server: Service Pack 1 (*10.1.0.622*), Service Pack 2;
  - Kaspersky Security для систем хранения данных Service Pack 1 (*10.1.0.622*);
  - Kaspersky Endpoint Security 10 для Mac: 10 Service Pack 1 (*10.1.0.622*), 10 Service Pack 1 (10.2.0.267).
- **Для виртуальных машин:**
  - Kaspersky Security для виртуальных сред 4.0 Легкий агент;
  - Kaspersky Security для виртуальных сред 4.0 Защита без агента Service Pack 1 (*4.1.0.47*);
  - Kaspersky Security для виртуальных сред 5.0 Легкий агент;
  - Kaspersky Security для виртуальных сред 5.1 Легкий агент;
  - Kaspersky Security для виртуальных сред 4.0 Защита без агента.
- **Для почтовых систем и серверов SharePoint / серверов совместной работы (централизованное развертывание не поддерживается):**
  - Kaspersky Security 8.0 для Linux Mail Server Maintenance Pack 2 (*8.0.2.16*);
  - Kaspersky Secure Mail Gateway 1.0, 1.1 (*1.1.0.379*), 1.1MR1 (*1.1.1.24*), 1.1MR2, 1.1MR3;
  - Kaspersky Security 9.0 for SharePoint Server: 9.0MR3 (*9.3.58811.0*);
  - Kaspersky Security 9.0 for Microsoft Exchange Servers: 9.0MR3 (*9.3.54.0*), 9.0MR4 (*9.4.189.0*),

9.0MR5.

- **Для обнаружения целевых атак:**
  - Платформа Kaspersky Anti Targeted Attack.

Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

В этом разделе

Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*). Серверы администрирования должны быть защищены от любого типа несанкционированного доступа, включая физическую защиту.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- под именем "Сервер администрирования Kaspersky Security Center";
- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью **Локальная система** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;
- обновление баз и модулей программ "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе программ "Лаборатории Касперского";
- распространение ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

Вы можете подключиться к Серверу администрирования с помощью Консоли администрирования (см. раздел "Сервер администрирования Kaspersky Security Center и Консоль администрирования" на стр. 64).

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию вида "главный сервер – подчиненный сервер". Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. раздел "*Виртуальный Сервер администрирования*" на стр. 35).

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).

- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить в каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

См. также:

Иерархия Серверов администрирования: Главный Сервер администрирования и подчиненный Сервер администрирования 68

Виртуальные Серверы администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент программы Kaspersky Security Center, предназначенный для управления сетью организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования использует для работы базу данных главного Сервера администрирования: задачи резервного копирования и восстановления данных, проверки и получения обновлений не поддерживаются на виртуальном Сервере.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки программ "Лаборатории Касперского" на клиентские устройства,

работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.

- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

Сервер мобильных устройств

Сервер мобильных устройств – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Существуют два вида Серверов мобильных устройств:

- Сервер мобильных устройств Exchange ActiveSync. Устанавливается на устройство, на котором установлен сервер Microsoft Exchange, и позволяет получать данные с сервера Microsoft Exchange и передавать их на Сервер администрирования. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими протокол Exchange ActiveSync.
- Сервер iOS MDM. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими сервис Apple® Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

Веб-сервер

Веб-сервер Kaspersky Security Center (далее также *Веб-сервер*) – это компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

При создании автономный пакет установки автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных пакетов установки. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере.

При создании iOS MDM-профиль для мобильного устройства пользователя также автоматически публикуется на Веб-сервере. Опубликованный профиль автоматически удаляется с Веб-сервера после успешной установки на мобильное устройство пользователя (см. раздел "Добавление мобильных устройств в список управляемых устройств" на стр. 693).

Папка общего доступа используется для размещения информации, доступной всем пользователям, устройства которых находятся под управлением Сервера администрирования. Если у пользователя нет прямого доступа к папке общего доступа, ему можно передать информацию из этой папки с помощью Веб-сервера.

Для передачи пользователям информации из папки общего доступа с помощью Веб-сервера администратору требуется создать в папке общего доступа вложенную папку public и поместить в нее информацию.

Синтаксис ссылки для передачи информации пользователю выглядит следующим образом:

```
https://<имя Веб-сервера>:<порт HTTPS>/public/<объект>
```

где:

- `<имя Веб-сервера>` – имя Веб-сервера Kaspersky Security Center.
- `<порт HTTPS>` – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию установлен порт 8061.
- `<объект>` – вложенная папка или файл, доступ к которым требуется открыть для пользователя.

Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на локальное устройство предназначенную для него информацию.

Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Kaspersky Security Center. Агент администрирования требуется установить на все устройства, на которых управление работой программ "Лаборатории Касперского" выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Агент администрирования Kaspersky Security Center 11";

- с автоматическим типом запуска при старте операционной системы;
- с помощью учетной записи LocalSystem.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*.

Агент администрирования можно установить на устройство под управлением операционной системы Windows, Linux или Mac. Вы можете активировать компонент следующими способами:

- Инсталляционный пакет в хранилище Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования).
- Инсталляционный пакет на веб-сервере "Лаборатории Касперского" (см. раздел "Получение актуальных версий программ" на стр.288).

Нет необходимости устанавливать Агент администрирования на устройства, на которых установлен Сервер администрирования, поскольку северная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования.

Название процесса, который запускает Агент администрирования, – *klnagent.exe*.

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (*периодический сигнал*) равным 15 минут на 10 000 управляемых устройств.

Группы администрирования

Группа администрирования (далее также *"группа"*) – это набор клиентских устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым.

Для всех клиентских устройств в группе устанавливаются:

- Единые параметры работы программ – с помощью групповых политик.
- Единый режим работы всех программ – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей программы, проверку устройства по требованию и включение постоянной защиты.

Клиентское устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и клиентские устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести компьютер этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, на компьютер будут автоматически переданы настойки программ, необходимые для позиции разработчика.

Управляемое устройство

Управляемое устройство – это устройство под управлением операционной системы Windows, Linux или Mac, расположенное в сети, в которой установлен Агент администрирования. Вы можете управлять такими устройствами с помощью задач и политик для программ, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 100 000 устройств.

Нераспределенное устройство

Нераспределенное устройство – это устройство в сети, которое не включено ни в одну из групп администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них программы.

Когда в сети обнаруживается новое устройство, оно относится в группу администрирования Нераспределенные устройства. Можно настроить правила автоматического распределения устройств по группам администрирования в момент обнаружения.

Рабочее место администратора

Устройства, на которых установлен компонент *Консоль администрирования*, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Найдите его в меню **Пуск** → **Программы** → **Kaspersky Security Center**.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Плагин управления

Управление программами "Лаборатории Касперского" через Консоль администрирования выполняется при помощи *плагинов управления*. В состав каждой программы "Лаборатории Касперского", которой можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления программой в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры программы, а также параметры задач этой программы;
- получать информацию о задачах программы, событиях в ее работе, а также о статистике работы программы, получаемой с клиентских устройств.

Политики

Политика – это набор параметров работы программы, определенный для группы администрирования (см. раздел "Группа администрирования" на стр. 38). Политика определяет не все параметры программы.

Для одной программы можно настроить несколько политик с различными значениями. Однако в каждый момент времени для программы может быть активна только одна политика в группе администрирования.

Вы можете активировать отключенную политику при возникновении определенного события. Это означает, например, что в период вирусных эпидемий можно включить параметры для более сильной антивирусной защиты.

Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Параметры программы определяются параметрами политик и задач.

Вложенные группы и подчиненные Серверы администрирования наследуют задачи групп более высоких уровней иерархии.

Параметр **Наследовать параметры родительской политики** находится в окне свойств унаследованной политики, в блоке **Наследование параметров** раздела **Общие**. В любое время можно отключить наследование из родительской политики, если эта возможность не заблокирована в политике верхнего уровня.

В разделе **Параметры программы** вы можете заблокировать параметры, которые требуется оставить без изменений в дочерних политиках. Каждый параметр, представленный в политике, имеет атрибут замок: . Значок "замка" показывает, можно ли изменять параметры политики в политиках более низких уровней иерархии (для вложенных групп и подчиненных Серверов администрирования). Если блокировка применяется к параметру групповой политики, нельзя переопределить значение этого параметра для вложенных подгрупп этой группы.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

О профилях политики

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам – не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Kaspersky Security Center позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

Задачи

Kaspersky Security Center управляет работой программ, установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Вы можете создать задачу для программы, только если для этой программы установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждой программы вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и в Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

Область действия задачи

Область задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Локальная задача. Область задачи – это само устройство.
- Задача Сервера администрирования. Область задачи – Сервер администрирования.
- Групповая задача. Область задачи – перечень устройств, входящих в группу.

При создании глобальной задачи можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка является наиболее гибким способом задания области действия задачи.

Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

Задачи будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Взаимосвязь политики и локальных параметров программы

При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров программы. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт замком).

Значение параметра, которое использует программа на клиентском устройстве (см. рис. ниже), определяется наличием замка (🔒) у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.

- Если запрет не наложен, то на каждом клиентском устройстве программа использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры программы.

Рисунок 1: Политика и локальные параметры программы

Таким образом, при выполнении задачи на клиентском устройстве программа использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами программы, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры программы изменяются после первого применения политики в соответствии с параметрами политики.

Точка распространения

Точка распространения (ранее называлась "Агент обновлений") – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в сети. Точка распространения может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае

для точки распространения, должна быть создана задача обновления (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства" на стр. 437).

Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.
- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования (см. раздел "Использование точек распространения в качестве шлюза" на стр. 538).

  Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, точку распространения можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

  Наличие точки распространения, работающей в режиме шлюза соединений, не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.
- Выполнять удаленную установку как сторонних программ, так и программ "Лаборатории Касперского" средствами Microsoft Windows, в том числе на клиентские устройства без установленного Агента администрирования.

  Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.
- Исполнять роль прокси-сервера, участвующего в Kaspersky Security Network.

  Можно включить прокси-сервер KSN на стороне точки распространения, чтобы устройство исполняло роль прокси-сервера KSN (см. раздел "Назначение устройства точкой распространения вручную" на стр. 379). В этом случае на устройстве запустится служба прокси-сервера KSN (ksnproxy) (см. раздел "Изменения в системе после установки Сервера администрирования на устройство" на стр. 208).

Передача файлов от Сервера администрирования точке распространения осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены точками распространения вручную администратором (см. раздел "Назначение устройства точкой распространения вручную" на стр. 379) или автоматически Сервером администрирования Полный список точек распространения для указанных групп администрирования отображается в отчете со списком точек распространения.

Областью действия точки распространения является группа администрирования, для которой она назначена администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Областью действия точек распространения также может являться сетевое местоположение. Сетевое местоположение используется для формирования вручную набора устройств, на которые точка распространения будет распространять обновления. Определение сетевого местоположения доступно только для устройств под управлением операционной системы Windows.

Если точки распространения назначаются автоматически Сервером администрирования, то Сервер назначает точки распространения по широковещательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковещательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковещательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковещательные домены каждые два часа. После того как точки распространения назначены по широковещательным доменам, их нельзя назначить снова по группам администрирования.

Если точки распространения назначаются администратором вручную, возможно назначение только по группам администрирования.

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.
Kaspersky Security Center присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов. Функция присвоения уникальных адресов работает в версиях Kaspersky Security Center 10 Service Pack 3 и выше. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях программы, изменены не будут.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

Статус точки распространения обновлений (*Активный* / *Резервный*) отображается флажком в отчете утилиты klnagchk (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Klnagchk utility" на стр. 593).

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Kaspersky Security Center создает инцидент с уровнем важности *Предупреждение*. Инцидент будет опубликован в свойствах устройства в разделе **Инциденты**.

При работе задач удаленной установки на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Устройства, выполняющие роль точек распространения, должны быть защищены от любого типа несанкционированного доступа, в том числе физически защищены.

Архитектура программы

Этот раздел содержит описание компонентов Kaspersky Security Center и их взаимодействия.

Программа Kaspersky Security Center включает в себя следующие основные компоненты:

- **Сервер администрирования** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.
- **Агент администрирования** (далее также *Агент*). Осуществляет взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft® Windows®. Для программ "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.
- **Консоль администрирования** (далее также *Консоль*). Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.
- **Сервер мобильных устройств**. Предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

См. также:

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Основной сценарий развертывания и другие сценарии развертывания

В этом разделе описаны принципы основного сценария развертывания Kaspersky Security Center и даны ссылки на другие сценарии развертывания. Следуя основному сценарию, вы можете развернуть Сервер администрирования, а также установить на устройства сети Агент администрирования и программы безопасности. Вы можете использовать этот сценарий и для ознакомления с программой, и для установки программы с целью дальнейшей работы.

Развертывание Kaspersky Security Center требует планирования ресурсов: установку Сервера администрирования, установку Агента администрирования и программ безопасности на клиентских устройствах, объединение устройств в группы администрирования.

Развертывание Kaspersky Security Center в облачном окружении (см. раздел "Сценарий:развертывание Kaspersky Security Center в облачном окружении" на стр. 768) и развертывание Kaspersky Security Center для поставщиков услуг описаны в соответствующих разделах справки.

В этом сценарии рекомендуется отвести на установку Сервера администрирования не менее часа, а на выполнение сценария целиком – не менее одного рабочего дня.

Развертывание Kaspersky Security Center состоит из следующих шагов:

a. **Выбор структуры защиты организации**

   Ознакомьтесь с компонентами Kaspersky Security Center (см. раздел "Архитектура" на стр. 48). Выберите структуру защиты (см. раздел "Выбор структуры защиты организации" на стр. 78) и конфигурацию сети (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 79) , наиболее подходящие для вашей организации Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам (см. раздел "Планирование развертывания Kaspersky Security Center" на стр. 76), если вы работаете с распределенной сетью.

   Для достижения и сохранения оптимальной производительности при различных условиях работы, пожалуйста, учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center (подробнее см. раздел "Руководство по масштабированию" на стр. 919).

   Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования (см. раздел "Иерархия Серверов администрирования" на стр. 34). Для этого нужно понять, возможно и целесообразно ли обслуживание всех клиентских устройств одним Сервером администрирования или требуется выстроить иерархию Серверов администрирования. Вам также может потребоваться выстроить иерархию Серверов администрирования, совпадающую с организационной структурой предприятия, сеть которого вы хотите защитить.

   Если вам требуется обеспечить защиту мобильных устройств, выполните подготовительные действия по настройке Сервера мобильных устройств Exchange ActiveSync (на стр. 98) и Сервера iOS MDM (на стр. 101).

   Убедитесь, что устройства, выбранные вами для использования в качестве Серверов

администрирования, а также для установки Консоли администрирования, соответствуют аппаратным и программным требованиям (на стр 23).

b. Подготовка к лицензированию Kaspersky Security Center

Если вы планируете использовать версию Kaspersky Security Center с поддержкой Управления мобильными устройствами, Интеграцией с SIEM-системами и / или с поддержкой Системного администрирования, убедитесь, что у вас имеется файл ключа либо код активации для лицензирования программы.

c. Подготовка к лицензированию управляемых программ защиты

Во время развертывания защиты вам потребуется предоставить "Лаборатории Касперского" активные ключи на те программы, которыми вы планируете управлять с помощью Kaspersky Security Center (см. список доступных для управления программ безопасности, раздел Программы "Лаборатории Касперского"). Централизованное развертывание" на стр. 271)). Подробнее о лицензировании каждой из программ безопасности вы можете прочитать в справках к этим программам.

d. Выбор аппаратной конфигурации Сервера администрирования и СУБД

Спланируйте аппаратную конфигурацию для СУБД и Сервера администрирования (см. раздел "Аппаратные требования для СУБД и Сервера администрирования" на стр. 840) с учетом количества устройств в вашей сети.

e. Выбор СУБД

При выборе СУБД (на стр. 82) учитывайте количество управляемых устройств, которые будет обслуживать Сервер администрирования. Если в вашей сети менее 10 000 устройств и вы не планируете увеличивать их количество, вы можете выбрать бесплатную СУБД SQL Express или MySQL и установить ее на одном устройстве с Сервером администрирования. Если в вашей сети более 10 000 устройств (или вы планируете расширение сети до такого количества устройств), рекомендуется выбирать платную СУБД SQL и размещать ее на отдельном устройстве. Платная СУБД может работать с несколькими Серверами администрирования, а бесплатная СУБД – только с одним.

f. Установка СУБД и создание базы данных

Узнайте больше об учетных записях для работы с СУБД (на стр. 179) и установите СУБД. Запишите и сохраните параметры СУБД, поскольку они потребуются вам при установке Сервера администрирования. Эти параметры включают имя SQL-сервера, номер порта для подключения к SQL-серверу, имя учетной записи и пароль для доступа к SQL-серверу.

По умолчанию инсталлятор Kaspersky Security Center создает базу данных для размещения информации Сервера администрирования (см. раздел "Шаг 9. Настройка параметров SQL-сервера" на стр. 196)", однако вы можете отказаться от ее создания и использовать другую базу данных. В этом случае убедитесь, что база данных создана, вы знаете ее имя, а учетная запись, под которой Сервер администрирования получит доступ к этой базе данных, будет иметь для нее роль db_owner.

При необходимости обратитесь за информацией к администратору СУБД.

g. Настройка портов

Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты открыты необходимые порты (см. раздел "Порты, используемые Kaspersky Security Center" на стр. 56).

Если требуется предоставить доступ к Серверу администрирования из интернета, настройте порты и параметры подключения в зависимости от конфигурации сети (см. раздел "Предоставление доступа к Серверу администрирования из интернета" на стр. 84).

h. Проверка учетных записей

Проверьте наличие у вас прав локального администратора для успешной установки Сервера администрирования Kaspersky Security Center и развертывания защиты на устройствах. Права локального администратора на клиентских устройствах нужны только для установки на эти устройства Агента администрирования. После установки Агента администрирования вы сможете с его помощью удаленно устанавливать программы на устройства, не пользуясь учетной записью с правами администратора устройства.

По умолчанию инсталлятор Kaspersky Security Center создает на устройстве, выбранном для установки Сервера администрирования, три локальные учетные записи, от имени которых будет запускаться Сервер администрирования (см. раздел "Шаг 6. Выбор учетной записи для запуска Сервера администрирования" на стр. 194) и службы Kaspersky Security Center (см. раздел "Шаг 7.Выбор учетной записи для запуска служб Kaspersky Security Center" на стр. 195):

- KL-AK-*: учетная запись службы Сервера администрирования;

- KlScSvc: учетная запись для прочих служб из состава Сервера администрирования;

- KlPxeUser: учетная запись для развертывания операционных систем.

Вы можете отказаться от создания учетных записей для служб Сервера администрирования и других служб. Вместо этого вы можете использовать существующие учетные записи, например учетные записи домена, если планируете установить Сервер администрирования на отказоустойчивом кластере (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. 183) или планируете использовать учетные записи домена вместо локальных учетных записей по другой причине. В этом случае убедитесь, что учетные записи для запуска Сервера администрирования и служб Kaspersky Security Center созданы, являются непривилегированными и обладают необходимыми правами для доступа к СУБД (см. раздел "Учетные записи для работы с СУБД" на стр. 179). (Если вы планируете в дальнейшем разворачивать операционные системы на устройствах средствами Kaspersky Security Center, не отказывайтесь от создания учетных записей (см. раздел "Развертывание операционных систем на новых устройствах в сети" на стр. 668).)

i. Установка Сервера администрирования, Консоли администрирования и плагинов управления для программ безопасности

Установите Сервер администрирования (см. раздел "Установка Kaspersky Security Center" на стр. 177) на устройство, которое вы выбрали (либо устройства, если вы планируете использовать более одного Сервера администрирования (см. раздел "Типовая конфигурация: один офис" на стр. 80)). Вы можете выбрать стандартную или выборочную установку Сервера администрирования. Вместе с Сервером администрирования установится Консоль администрирования.

Стандартная установка (на стр. 185) рекомендуется, если вы хотите ознакомиться с программой

Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор модулей управления, заданный по умолчанию, для программ "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

Выборочная установка (на стр. 190) рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в неинтерактивном режиме (см. раздел "Установка в неинтерактивном режиме" на стр. 200).

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования.

При необходимости можно установить Консоль администрирования (см. раздел "Установка Консоли администрирования на рабочее место администратора" на стр. 207) на рабочее место администратора независимо для управления Сервером администрирования по сети.

j. Первоначальная настройка и лицензирование

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 213). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (на стр. 40) и задачи (на стр. 41) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. раздел "Сценарий: Настройка защиты сети" на стр. 305).

Если вы планируете использовать функциональность, выходящую за рамки Базовой функциональности, активируйте программу по лицензии (см. раздел "Об ограничениях базовой функциональности" на стр. 259). Вы можете выполнить это на одном из шагов мастера первоначальной настройки (см. раздел "Шаг 2. Выбор способа активации программы" на стр. 215).

k. Обнаружение устройств в сети

Этот шаг входит в мастер первоначальной настройки (см. раздел "Шаг 10. Обнаружение устройств" на стр. 225). Вы можете также запустить обнаружение устройств (на стр. 238) вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

l. Проверка успешности установки Сервера администрирования

После успешного выполнения предыдущих шагов Сервер администрирования установлен и готов к дальнейшей работе.

Убедитесь, что работает Консоль администрирования и что вы можете подключиться через Консоль к Серверу администрирования. Убедитесь также, что на Сервере администрирования имеется задача загрузки обновлений в хранилище Сервера администрирования (в папке **Задачи** дерева консоли) и политика для Kaspersky Endpoint Security (в папке **Политики** дерева консоли).

После завершения проверки, перейдите к шагам ниже.

m. Установка Агента администрирования и программ безопасности на устройства в сети

Развертывание защиты (см. раздел "Сценарий:Настройка защиты сети" на стр 305) в сети организации подразумевает установку Агента администрирования и программ безопасности (например, Kaspersky Endpoint Security для Windows) на устройства, которые были обнаружены Сервером администрирования при обнаружении устройств.

Программы безопасности защищают устройства от вирусов и / или других программ, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

Перед тем как установить Агент администрирования и программы безопасности на устройства в сети, убедитесь, что эти устройства доступны (включены).

Возможна удаленная или локальная установка программ безопасности и Агента администрирования.

Удаленная установка (см. раздел "Программы "Лаборатории Касперского".Централизованное развертывание" на стр. 271) – с помощью мастера развертывания защиты вы можете удаленно установить программу безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования на устройствах, которые были обнаружены Сервером администрирования в сети организации. Как правило, задача удаленной установки успешно развертывает защиту для большинства сетевых устройств. Однако она может возвращать ошибку на некоторых устройствах, если, например, устройство отключено или недоступно по другой причине. В этом случае рекомендуется вручную подключиться к устройству и использовать локальную установку.

Локальная установка (см. раздел "Локальная установка программ" на стр. 138) – используется на тех устройствах сети, на которых не удалось развернуть защиту с помощью задачи удаленной установки. Чтобы установить защиту на такие устройства, создайте автономный пакет установки для запуска на этих устройствах локально.

Установка Агента администрирования на устройства с операционными системами Linux и MacOS описана в документации для Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac соответственно. (Несмотря на то, что устройства под управлением операционных систем Linux и MacOS считаются менее уязвимыми, чем устройства под управлением Windows, на них также рекомендуется устанавливать программы безопасности.)

После установки убедитесь, что программа безопасности установлена на управляемые устройства. Для этого запустите Отчет о версиях программ "Лаборатории Касперского" и ознакомьтесь с его результатами (см. Раздел "Просмотр реестра программ" на стр. 397).

n. Распространение лицензионных ключей на клиентские устройства

Распространите лицензионные ключи на клиентские устройства, чтобы активировать управляемые программы безопасности на этих устройствах (см. раздел "Программы "Лаборатории Касперского":

лицензирование и активация" на стр. 295).

o. **Настройка защиты мобильных устройств**

Этот шаг входит в мастер первоначальной настройки.

Если вы хотите управлять корпоративными мобильными устройствами, разверните Управление мобильными устройствами (см. раздел "Развертывание систем управления мобильными устройствами" на стр. 149).

p. **Создание структуры групп администрирования**

В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования с учетом организационной структуры организации (см. раздел "Настройка точек распространения и шлюзов соединений" на стр. 534). Вы можете создать правила перемещения для распределения устройств по группам или распределить устройства вручную (см. раздел "Правила перемещения устройств" на стр. 349). Для групп администрирования можно назначать групповые задачи, определять область действия политик и назначать точки распространения.

Убедитесь, что все управляемые устройства правильно распределены по соответствующим группам администрирования и что у вас в сети не осталось нераспределенных устройств (на стр. 237).

q. **Назначение точек распространения**

Точки распространения (см. Раздел "О точках распространения" на стр. 86)для групп администрирования назначаются автоматически, но при необходимости вы можете назначить их вручную. Точки администрирования рекомендуется использовать в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью.

Результаты

После завершения сценария в сети организации будет развернута защита:

- Установлена СУБД для Сервера администрирования.
- Установлен Сервер администрирования Kaspersky Security Center.
- Созданы необходимые политики и задачи, а также настроены заданные по умолчанию параметры политик и задач.
- На управляемые устройства установлены программы безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования.
- Созданы группы администрирования (возможно, объединенные в иерархию).
- При необходимости развернута защита мобильных устройств.
- При необходимости назначены точки распространения.

См. также:

Порты, используемые Kaspersky Security Center

В следующей таблице перечислены порты, которые должны быть открыты на Серверах администрирования и на клиентских устройствах.

Таблица 1. Порты, используемые Kaspersky Security Center

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (за исключением UDP-портов)	Назначение порта	Область
Сервер администрирования	8060	klcsweb	TCP	Нет	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов
	8061	klcsweb	TCP	Да	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (за исключением UDP-портов)	Назначение порта	Область
	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования и от подчиненных Серверов администрирования; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Управление клиентскими устройствами и подчиненными Серверами администрирования
	13000	klserver	UDP	Нет значения	Прием информации от Агентов администрирования о выключении устройств	Управление клиентскими устройствами
	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования	Управление Сервером администрирования

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (за исключением UDP-портов)	Назначение порта	Область
	13292	*klserver*	*TCP*	*Да*	*Прием подключений от мобильных устройств*	*Управление мобильными устройствами*
	*13294**	*klserver*	*TCP*	*Да*	*Прием подключений от устройств с защитой на уровне UEFI*	*Управление клиентскими устройствами с защитой на уровне UEFI*
	14000	klserver	TCP	Нет	Прием подключений от Агентов администрирования	Управление клиентскими устройствами
	*13111**	*ksnproxy*	*TCP*	*Нет*	*Прием запросов от управляемых устройств к прокси-серверу KSN*	*Прокси-сервер KSN*
	*15111**	*ksnproxy*	*UDP*	*Нет значения*	*Прием запросов от управляемых устройств к прокси-серверу KSN*	*Прокси-сервер KSN*
	17000	klactprx	TCP	Да	Прием подключений для активации программ от управляемых устройств (кроме мобильных устройств)	Прокси-сервер активации для немобильных устройств

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (за исключением UDP-портов)	Назначение порта	Область
	*17100**	*klactprx*	*TCP*	*Да*	*Прием подключений для активации приложений от мобильных устройств*	*Прокси-сервер активации для мобильных устройств*
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования	Доставка обновлений и инсталляционных пакетов
Точка распространения	15001	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования	Доставка обновлений и инсталляционных пакетов
	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов
Сервер iOS MDM	*443**	*kliosmdmservicesrv*	*TCP*	*Да*	*Прием соединений от мобильных устройств iOS*	*Управление мобильными устройствами*

Курсивом обозначены порты, которые потребуется открыть, только если вы работаете с мобильными устройствами (см. графы "Назначение порта" и "Область").

Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server, или порт 1433 для Microsoft SQL Server; пожалуйста, подробную информацию см. в документации СУБД).

См. также:

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения

В этом разделе приведены схемы взаимодействия между компонентами в составе Kaspersky Security Center и управляемыми программами безопасности. На схемах приведены номера портов, которые должны быть доступны, и имена процессов, открывающих порты.

В этом разделе

Условные обозначения в схемах взаимодействия

В таблице ниже приведены условные обозначения, использованные в схемах.

Таблица 2. Условные обозначения

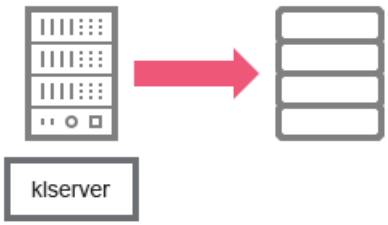
Иконка	Пояснение
	Сервер администрирования

	Подчиненный Сервер администрирования
	СУБД
	Клиентское устройство, на котором установлены Агент администрирования и программа семейства Kaspersky Endpoint Security (либо другая программа безопасности, которой может управлять Kaspersky Security Center)
	Шлюз соединения
	Точка распространения
	Мобильное клиентское устройство с установленной программой Kaspersky Security для мобильных устройств
	Браузер на устройстве пользователя
	Процесс, запущенный на устройстве и открывающий какой-либо порт
	Порт и его номер
	Трафик TCP (направление стрелки обозначает направление трафика)
	Трафик UDP (направление стрелки обозначает направление трафика)
	Вызов COM
	Транспорт СУБД

	Границы демилитаризованной зоны

Сервер администрирования и СУБД

Данные от Сервера администрирования поступают в базу данных SQL Server или MySQL.



Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server, или порт 1433 для Microsoft SQL Server; пожалуйста, подробную информацию см. в документации СУБД).

См. также:

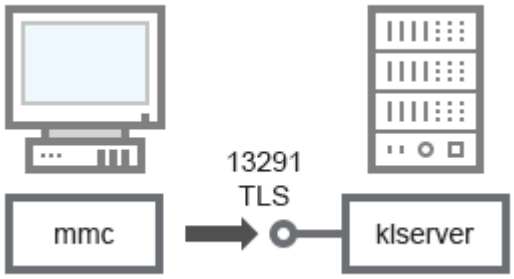
Условные обозначения в схемах взаимодействия 61

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Порты, используемые Kaspersky Security Center 56

О выборе СУБД для Сервера администрирования 82

Сервер администрирования и Консоль администрирования



Пояснения к схеме см. в таблице ниже.

Таблица 3. Сервер администрирования и Консоль администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13291	klserver	TCP	Да	Прием подключений от Консоли администрирования

См. также:

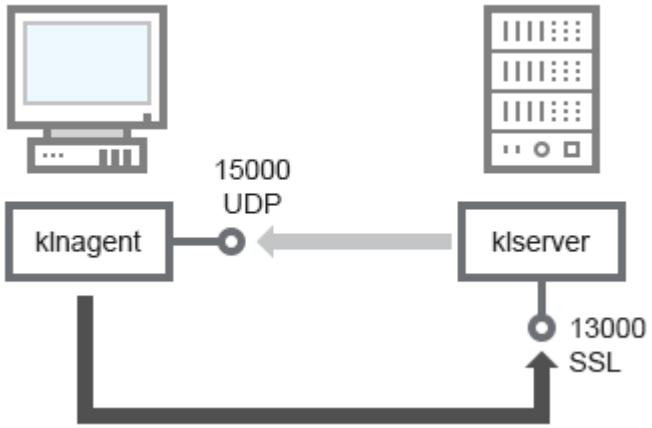
Условные обозначения в схемах взаимодействия 61

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

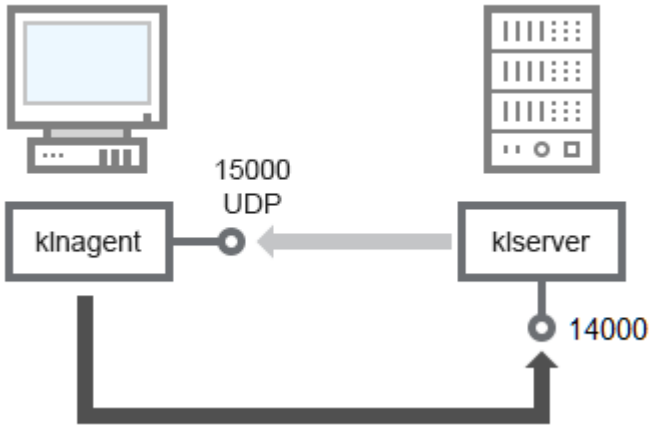
Порты, используемые Kaspersky Security Center 56

Сервер администрирования и клиентское устройство: Управление программой безопасности

Сервер администрирования принимает подключения от Агентов администрирования по защищенному порту 13000 (см. рис. ниже).



Если вы использовали Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключения от Агентов администрирования по незащищенному порту 14000 (см. рис. ниже). Kaspersky Security Center 11 также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.



Пояснения к схемам см. в таблице ниже.

Таблица 4. Сервер администрирования и клиентское устройство: Управление программой безопасности (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования
Сервер администрирования	14000	klserver	TCP	Нет	Прием подключений от Агентов администрирования

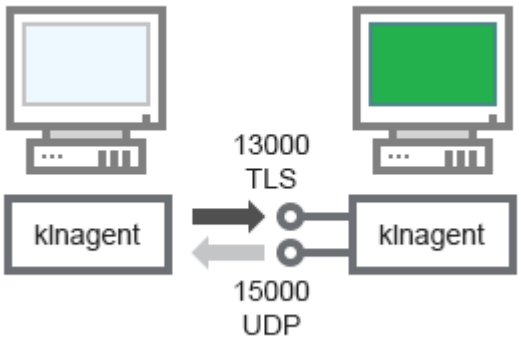
См. также:

Условные обозначения в схемах взаимодействия 61

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Порты, используемые Kaspersky Security Center 56

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения



Пояснения к схеме см. в таблице ниже.

Таблица 5. Обновление программного обеспечения с помощью точки распространения (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS (только для TCP)	Назначение порта
Агент администрирования	15000	klnagent	UDP	Нет значения	Многоадресная рассылка Агентам администрирования
Точка распространения	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также:

Условные обозначения в схемах взаимодействия 61

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

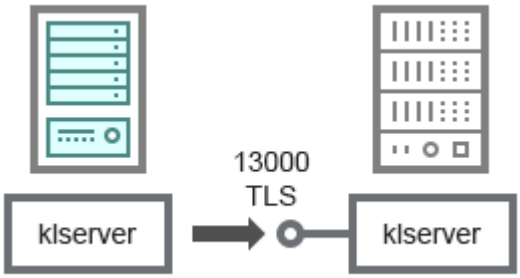
Порты, используемые Kaspersky Security Center 56

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

На схеме (см. рис. ниже) показано, как используется порт 13000 для взаимодействия Серверов администрирования, объединенных в иерархию.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" на стр. 542). Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 64).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.



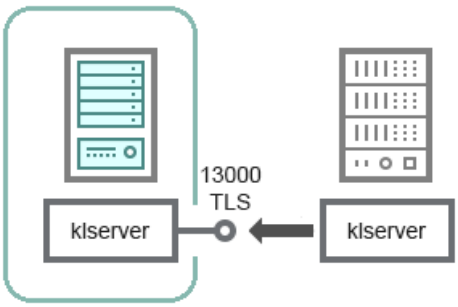
Пояснения к схеме см. в таблице ниже.

Таблица 6. Иерархия Серверов администрирования (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Главный Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от подчиненных Серверов администрирования

См. также:

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен (см. раздел "Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования" на стр. 542). Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 64).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.

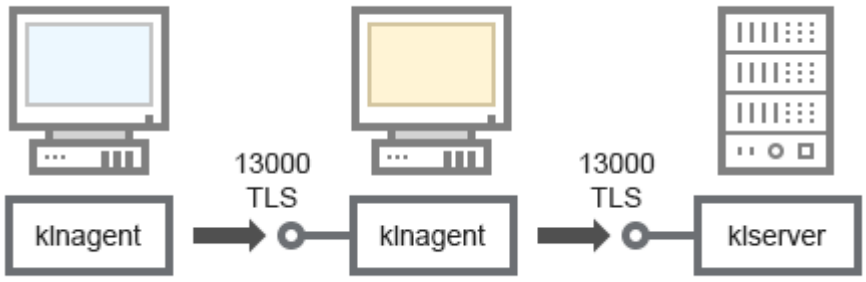
Таблица 7. Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Подчиненный Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от главного Сервера администрирования

См. также:

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



Пояснения к схеме см. в таблице ниже.

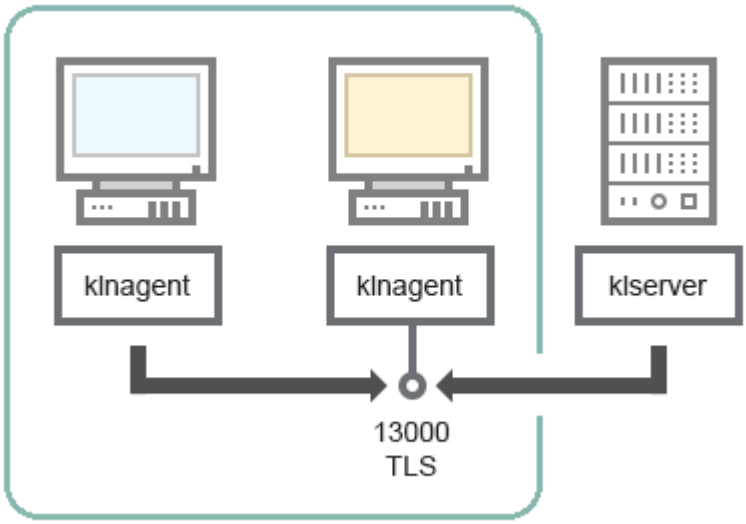
Таблица 8. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13000	klserver	TCP	Да	Прием подключений от Агентов администрирования

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также:

Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство



Пояснения к схеме см. в таблице ниже.

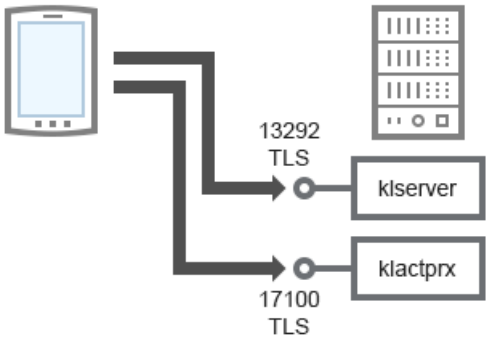
Таблица 9. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Агент администрирования	13000	klnagent	TCP	Да	Прием подключений от Агентов администрирования

См. также:

Активация и управление приложением безопасности на мобильном устройстве



Пояснения к схеме см. в таблице ниже.

Таблица 10. Активация и управление приложением безопасности на мобильном устройстве (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	13292	klserver	TCP	Да	Прием подключений от Консоли администрирования к Серверу администрирования

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	TLS	Назначение порта
Сервер администрирования	17100	klserver	TCP	Да	Прием подключений для активации приложений от мобильных устройств

См. также:

Условные обозначения в схемах взаимодействия 61

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Порты, используемые Kaspersky Security Center 56

Развертывание системы управления по протоколу Exchange ActiveSync 149

Лучшие практики развертывания

Kaspersky Security Center является распределенной программой. В состав Kaspersky Security Center входят следующие программы:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Агент администрирования – служит для управления установленной на устройстве программой безопасности, а также для получения информации об устройстве и передаче этой информации на Сервер администрирования. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и программы безопасности на устройства организации.

В этом разделе

Подготовка к развертыванию

В этом разделе описаны шаги, которые вы должны выполнить перед развертыванием Kaspersky Security Center.

В этом разделе

Планирование развертывания Kaspersky Security Center

Этот раздел содержит информацию об оптимальных вариантах развертывания компонентов Kaspersky Security Center в сети организации в зависимости от различных факторов:

- общего количества устройств;
- наличия организационно или географически обособленных подразделений (офисов, филиалов);
- наличия обособленных сетей, связанных узкими каналами;
- необходимости доступа к Серверу администрирования из интернета.

В этом разделе

Типовые способы развертывания системы защиты

В этом разделе описаны типовые способы развертывания системы защиты в сети организации с помощью Kaspersky Security Center.

Необходимо обеспечить защиту системы от несанкционированного доступа всех видов. Перед установкой программы на устройство рекомендуется установить все доступные обновления безопасности для операционной системы и обеспечить физическую защиту Серверов администрирования и точек распространения.

Вы можете развернуть систему защиты в сети организации с помощью Kaspersky Security Center, используя следующие схемы развертывания:

- Развертывание системы защиты средствами Kaspersky Security Center через Консоль администрирования.

  Установка программ "Лаборатории Касперского" на клиентские устройства и подключение клиентских устройств к Серверу администрирования происходит автоматически с помощью Kaspersky Security Center.

  Основной схемой развертывания является развертывание системы защиты через Консоль администрирования.

- Развертывание системы защиты вручную с помощью автономных пакетов установки, сформированных в Kaspersky Security Center.

  Установка программ "Лаборатории Касперского" на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

  Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Active Directory®.

Общая информация о планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 100 000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

Если в составе организации есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В противном случае такие офисы следует рассматривать как обособленные сети, связанные узкими каналами, см. раздел "Типовая конфигурация: несколько крупных офисов с собственными администраторами" (на стр. 80).

При наличии обособленных сетей, связанных узкими каналами, в целях экономии трафика в таких сетях следует назначить один или несколько Агентов администрирования точками распространения (см. таблицу для расчета количества точек распространения, в разделе "Расчет количества и конфигурации точек распространения" на стр. 88). В этом случае все устройства обособленной сети будут получать обновления с таких "локальных центров обновлений". Точки распространения могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов "Лаборатории Касперского", см. раздел "Типовая конфигурация: множество небольших удаленных офисов

(на стр. 81)").

В разделе "Типовые конфигурации Kaspersky Security Center" на стр. 79 приведены подробные описания типовых конфигураций Kaspersky Security Center. При планировании развертывания следует, в зависимости от структуры организации, выбрать наиболее подходящую типовую конфигурацию.

На этапе планирования развертывания следует рассмотреть необходимость задания Серверу администрирования специального сертификата X.509. Задание сертификата X.509 для Сервера администрирования может быть целесообразно в следующих случаях (неполный список):

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для интеграции с инфраструктурой открытых ключей (PKI) организации;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

- Топология сети организации.
- Организационная структура.
- Число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними.
- Аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой.
- Пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации.
- Допустимое время выполнения важных административных операций в сети организации. К важным административным операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств.

При выборе структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
   - число сегментов сети;
   - скорость каналов связи между отдельными сегментами сети;
   - число управляемых устройств в каждом из сегментов сети;
   - пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты.
2. Определить допустимое время выполнения ключевых операций администрирования для всех

управляемых устройств.

3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования (см. раздел "Нагрузка на сеть" на стр. 93). На основании проведенного анализа ответить на следующие вопросы:

   - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
   - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
   - Требуется ли использование точек распространения для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы вы можете составить набор допустимых структур защиты организации.

В сети организации можно использовать одну из следующих типовых структур защиты:

- Один Сервер администрирования. Все клиентские устройства подключены к одному Серверу администрирования. Роль точки распространения выполняет Сервер администрирования.
- Один Сервер администрирования с точками распространения. Все клиентские устройства подключены к одному Серверу администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.
- Иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль точки распространения выполняет главный Сервер администрирования.
- Иерархия Серверов администрирования с точками распространения. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.

См. также:

Типовая конфигурация точек распространения:один офис 535
Типовая конфигурация:несколько крупных офисов с собственными администраторами" 80
Типовая конфигурация:Множество небольших изолированных офисов 81

Типовые конфигурации Kaspersky Security Center

В этом разделе описаны следующие типовые конфигурации размещения компонентов Kaspersky Security Center в сети организации:

- один офис
- несколько крупных географически распределенных офисов с собственными администраторами;

- множество небольших географически распределенных офисов.

В этом разделе

Типовая конфигурация: один офис

В сети организации может быть размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества управляемых устройств (см. раздел "Аппаратные требования для СУБД и Сервера администрирования" на стр. 840).

Один Сервер администрирования может обслуживать до 100 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

Серверы администрирования могут быть размещены как во внутренней сети, так и в демилитаризованной зоне, в зависимости от того, нужен ли доступ к Серверам администрирования из интернета.

Если Серверов несколько, рекомендуется объединить их в иерархию. Наличие иерархии Серверов администрирования позволяет избежать дублирования политик и задач, работать со всем множеством управляемых устройств, как если бы они все управлялись одним Сервером администрирования: выполнять поиск устройств, создавать выборки устройств, создавать отчеты.

См. также:

Типовая конфигурация: несколько крупных офисов с собственными администраторами

При наличии нескольких крупных удаленных офисов следует рассмотреть возможность размещения Серверов администрирования в каждом из офисов, по одному или по несколько Серверов администрирования в каждом, в зависимости от количества клиентских устройств и доступного аппаратного обеспечения. В таком случае каждый из офисов может быть рассмотрен как "Типовая конфигурация: один офис (на стр. 80)". Для упрощения администрирования все Серверы администрирования следует объединить в иерархию, возможно, многоуровневую.

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать правила переключения Агента администрирования между Серверами администрирования.

См. также:

Настройка профилей соединения для автономных пользователей 226

Типовая конфигурация:один офис 80

Порты, используемые Kaspersky Security Center 56

Типовая конфигурация: множество небольших удаленных офисов

Эта типовая конфигурация предусматривает один главный офис и множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Возможно, каждый из удаленных офисов находится за Network Address Translation (далее также NAT), то есть подключение из одного удаленного офиса в другой невозможно, офисы изолированы друг от друга.

В главном офисе следует поместить Сервер администрирования, а в остальных офисах назначить по одной или по несколько точек распространения. Так как связь между офисами осуществляется через интернет, целесообразно создать для точек распространения задачу Загрузка обновлений в хранилища точек распространения, так, чтобы точки распространения загружали обновления не с Сервера администрирования, а непосредственно с серверов "Лаборатории Касперского" (см. раздел "Создание задачи загрузки обновлений в хранилища точек распространения" на стр. 368).

Если в удаленном офисе часть устройств не имеет прямого доступа к Серверу администрирования (например, доступ к Серверу администрирования осуществляется через интернет, но доступ в интернет есть не у всех устройств), то точки распространения следует переключить в режим шлюза. В таком случае Агенты администрирования на устройствах в удаленном офисе будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть в удаленном офисе, целесообразно возложить выполнение этой функции на одну из точек распространения.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в удаленном офисе. Для решения этой проблемы целесообразно включить в свойствах устройств, являющихся точками распространения, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**). Этот режим доступен, если общее количество точек распространения не превышает 300.

См. также:

О точках распространения 86

Предоставление доступа к Серверу администрирования из интернета 84

Порты, используемые Kaspersky Security Center 56

О выборе СУБД для Сервера администрирования

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

SQL Server Express Edition ограничен по количеству используемой памяти, по количеству используемых ядер процессора и по максимальному размеру базы данных. Поэтому SQL Server Express Edition не может использоваться, если Сервер администрирования обслуживает более 10 000 устройств, либо если на управляемых устройствах используется компонент Контроль программ.

Если Сервер администрирования обслуживает более 10 000 устройств, рекомендуется использовать SQL Server с меньшими ограничениями, например: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition, SQL Server Enterprise Edition.

Если Сервер администрирования обслуживает не более 10 000 устройств и если на управляемых устройствах не используется компонент Контроль программ, вы можете использовать в качестве СУБД также MySQL 5.5, 5.6, 5.7. Не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5.

См. также:

Аппаратные требования для СУБД и Сервера администрирования 840

Выбор СУБД 82

Выбор СУБД

В процессе инсталляции Сервера администрирования необходимо выбрать СУБД, которую будет использовать Сервер администрирования. При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

В таблице ниже перечислены допустимые варианты СУБД и ограничения их использования.

Таблица 11. Ограничения СУБД

СУБД	Ограничения

СУБД	Ограничения
SQL Server Express Edition 2008 и выше	Не рекомендуется, если планируется обслуживание одним Сервером администрирования более 10 000 устройств или использование компонента Контроль программ.
Локальный SQL Server Edition, отличный от Express, 2008 и выше	Нет ограничений.
Удаленный SQL Server Edition, отличный от Express, 2008 и выше	Допустимо только в случае, если оба устройства находятся в одном домене Windows®; если домены разные, то между ними должно быть установлено двустороннее отношение доверия.
Локальный или удаленный MySQL 5.5, 5.6 или 5.7 (версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 и 5.5.5 не поддерживаются)	Не рекомендуется, если планируется обслуживание одним Сервером администрирования более 10 000 устройств или использование компонента Контроль программ.

Недопустимо совместное использование СУБД Server Express Edition Сервером администрирования и какой-либо другой программой.

См. также:

О выборе СУБД для Сервера администрирования 82

Учетные записи для работы с СУБД 179

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. В программе Kaspersky Security Center 10 Service Pack 1 и выше поддерживаются следующие возможности по управлению KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - статусы, события, отчеты и прочее;
  - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Обслуживание KES-устройств осуществляется Сервером администрирования по протоколу TLS, порт TCP 13292.

См. также:

Предоставление доступа к Серверу администрирования из интернета 84

Предоставление доступа к Серверу администрирования из интернета

В ряде случаев необходимо предоставить доступ к Серверу администрирования из интернета:

- для управления устройствами (ноутбуками) автономных пользователей;
- для управления устройствами, находящимися в удаленных офисах;
- при взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах;
- для управления мобильными устройствами.

В этом разделе рассмотрены типичные способы обеспечения доступа к Серверу администрирования из интернета. Во всех случаях предоставления доступа к Серверу администрирования из интернета может понадобиться задать Серверу администрирования специальный сертификат.

В этом разделе

Доступ из интернета:Сервер администрирования в локальной сети 84

Доступ из интернета: Сервер администрирования в демилитаризованной зоне (DMZ).....84

Доступ из интернета:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне 85

Доступ из интернета: Сервер администрирования в локальной сети

Если Сервер администрирования располагается во внутренней сети организации, с помощью механизма "Port Forwarding" порт Сервера администрирования 13000 TCP делается доступным извне. Если требуется управление мобильными устройствами, то делается доступным извне порт 13292 TCP.

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

Если Сервер администрирования располагается в демилитаризованной зоне сети организации, у него отсутствует доступ во внутреннюю сеть организации. Как следствие, возникают следующие ограничения:

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.
- Сервер администрирования не может выполнять первоначальное развертывание Агента

администрирования посредством принудительной инсталляции на устройства внутренней сети организации.

Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка программы безопасности уже могут быть выполнены Сервером администрирования. Однако первоначальное развертывание Агентов администрирования может быть выполнено иными средствами, например, при помощи групповых политик Microsoft® Active Directory®.

- Сервер администрирования не может посылать управляемым устройствам уведомления на порт 15000 UDP, что не является критичным для работы Kaspersky Security Center.
- Сервер администрирования не может опрашивать Active Directory. Однако результаты опроса Active Directory не нужны в большинстве сценариев.

Если описанные выше ограничения критичны, они могут быть сняты при помощи точек распространения, размещенных в сети организации:

- Для выполнения первоначального развертывания на устройствах без Агента администрирования следует предварительно установить Агент администрирования на одно из устройств и назначить это устройство точкой распространения. В результате первоначальная установка Агента администрирования на прочие устройства будет выполняться Сервером администрирования через эту точку распространения.
- Для обнаружения новых устройств во внутренней сети организации и для опроса Active Directory следует на одной из точек распространения включить желаемые виды опроса сети.
- Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия точками распространения. В свойствах назначенных точках распространения следует установить флажок **Не разрывать соединение с Сервером администрирования**. В результате Сервер администрирования будет иметь постоянную связь с точками распространения, а точки распространения смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (см. раздел "О точках распространения" на стр. 86).

Доступ из интернета: Использовать в качестве шлюза соединений в демилитаризованной зоне

Описанный ниже режим доступа применим для Kaspersky Security Center 10 Service Pack 1 и более поздних версий.

Сервер администрирования может располагаться во внутренней сети организации, а в демилитаризованной зоне сети может находиться устройство с Агентом администрирования, работающим в качестве шлюза соединений с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить Агент администрирования. При установке Агента администрирования в окне мастера установки **Шлюз**

соединений выбрать вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**. Использование устройств в качестве шлюза соединений доступно только для устройств под управлением Windows.

- На Сервере администрирования следует создать отдельную группу администрирования, в свойствах которой назначить по адресу в качестве шлюза соединений указанное выше устройство из демилитаризованной зоны. В эту группу администрирования не следует добавлять какие-либо устройства.
- Для Агентов администрирования, обращающихся к Серверу администрирования из интернета, при установке следует указать созданный выше шлюз соединений с помощью параметра **Подключаться к Серверу администрирования через шлюз соединений**.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

О точках распространения

Устройство с установленным Агентом администрирования может быть использовано в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае для устройства, являющегося точкой распространения, должна быть создана задача Загрузка обновлений в хранилища точек распространения (см. раздел "Создание задачи загрузки обновлений в хранилища точек распространения" на стр. 368).

- Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшить нагрузку на Сервер администрирования.
- Оптимизировать трафик.
- Предоставить Серверу администрирования доступ к устройствам в труднодоступных частях сети организации. Наличие точки распространения в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
  - отправлять устройствам уведомления по UDP;
  - опрашивать сеть;

- выполнять первоначальное развертывание.

Точка распространения назначается на группу администрирования. В этом случае областью действия точки распространения будут устройства, находящиеся в этой группе администрирования и всех ее подгруппах. При этом устройство, являющееся точкой распространения, не обязано находиться в группе администрирования, на которую она назначена.

Вы можете назначить точку распространения шлюзом соединений. В этом случае находящиеся в ее области действия устройства будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между устройствами с Агентом администрирования и Сервером администрирования невозможно прямое соединение.

См. также:

Настройка точек распространения и шлюзов соединений.....534

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим" (см. раздел "Требования для точки распространения" на стр. 842).

Таблица 12. Число уникально назначенных точек распространения в сети, содержащей один сегмент, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10,000 + 1), рекомендуется: (N/5,000 + 2), где N количество устройств в сети

Таблица 13. Число уникально назначенных точек распространения в сети, содержащей несколько сегментов, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 100	1
Более 100	Приемлемо: (N/10,000 + 1), рекомендуется: (N/5,000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Таблица 14. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Таблица 15. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 30	1
31 – 300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

См. также:

Типовая конфигурация:Множество небольших изолированных офисов 81

Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Виртуальные Серверы администрирования

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более

функциональна и предоставляет большую степень изоляции. Помимо собственной структуры групп администрирования для распределенных устройств с политиками и задачами, каждый виртуальный Сервер администрирования имеет также собственную группу нераспределенных устройств, собственные наборы отчетов, выборок устройств и событий, инсталляционных пакетов, правил перемещения устройств и так далее. Функциональность виртуальных Серверов администрирования может быть использована как сервис-провайдерами (xSP) для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра приложений и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на устройства сети организации wim-образы настольных и серверных версий операционных систем Windows®.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного устройства.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на "чистое" устройство, то есть на устройство без установленной на нем операционной системы;
- развертывание на устройство, работающее под управлением операционной системы Windows.

В составе Сервера администрирования неявно присутствует служебный образ WinPE (Windows Preinstallation Environment), который всегда используется как при захвате, так и во время развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех устройств. Как правило, требуется добавить драйверы чипсета, необходимые для работы сетевого интерфейса Ethernet.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK)

версии 2.0 и выше или Windows Assessment and Deployment Kit (WADK). Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.

- В сети, в которой расположено устройство, должен присутствовать DHCP-сервер.
- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится устройство. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KlPxeUser (эта учетная запись создается автоматически на этапе работы инсталлятора Сервера администрирования). Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки администратор должен явно указать архитектуру процессора устройства: x86 или x86-64.

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

Таблица 16. Ограничения Kaspersky Security Center

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные (стационарные) устройства)	10 000
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства

Тип ограничения	Значение
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- Первоначальное развертывание антивирусной защиты
- Первоначальное обновление антивирусных баз
- синхронизация клиентского устройства с Сервером администрирования;
- регулярное обновление антивирусных баз;
- обработка событий на клиентских устройствах Сервером администрирования.

В этом разделе

Первоначальное развертывание антивирусной защиты

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии 11 и Kaspersky Endpoint Security 11 для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем форсированной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security 11 для Windows, используя соединение с Сервером администрирования.

Таблица 17. Расход трафика

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security 11 для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security 11 для Windows

Сценарий	Установка Агента администрирования для одного клиентского устройства	Установка Kaspersky Endpoint Security 11 для Windows для одного клиентского устройства (с обновленными базами)	Совместная установка Агента администрирования и Kaspersky Endpoint Security 11 для Windows
Трафик от клиентского устройства к Серверу администрирования, КБ	1087,83	5564,49	6179,68
Трафик от Сервера администрирования к клиентскому устройству, КБ	38 835.86	203 366.39	242 536.62
Общий трафик (для одного клиентского устройства), КБ	39 923.70	208 930.88	248 716.31

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования точкой распространения. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты будут разосланы всем включенным устройствам в группе администрирования один раз. Таким образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком загрузки инсталляционных пакетов с Сервера администрирования. При этом источником инсталляционных пакетов является точка распространения, а не Сервер администрирования.

Первоначальное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при первом запуске задачи обновления баз на клиентском устройстве (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Таблица 18. Расход трафика

Сценарий	Первоначальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	80,0
Трафик от Сервера администрирования к клиентскому устройству, КБ	61,2

Сценарий	Первоначальное обновление антивирусных баз
Общий трафик (для одного клиентского устройства), КБ	141,2

Синхронизация клиента с Сервером администрирования

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Таблица 19. Расход трафика

Сценарий	Трафик от клиентских устройств к Серверу администрирования, КБ	Трафик от Сервера администрирования к клиентским устройствам, КБ	Общий трафик (для одного клиентского устройства), КБ
Первоначальная синхронизация до обновления баз на клиентском устройстве	368,6	463,7	832,3
Первоначальная синхронизация после обновления баз на клиентском устройстве	1 748,3	34 388,3	36 136,6
Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования	8,7	6,6	15,3
Синхронизация при изменении одного параметра в политике группы	11,1	13,3	24,4
Синхронизация при изменении одного параметра в групповой задаче	10,0	12,5	22,5

Принудительная синхронизация при отсутствии изменений на клиентском устройстве	47,3	15,5	62,8

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и программы безопасности;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

Добавочное обновление антивирусных баз

В этом разделе приведена информация о расходе трафика при инкрементальном обновлении антивирусных баз через 20 часов после предыдущего обновления (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Таблица 20. Расход трафика

Сценарий	Инкрементальное обновление антивирусных баз
Трафик от клиентского устройства к Серверу администрирования, КБ	436,9
Трафик от Сервера администрирования к клиентскому устройству, КБ	9 979,2
Общий трафик (для одного клиентского устройства), КБ	10 416,1

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Обработка событий клиентов Сервером администрирования

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события "Найден вирус", информация о котором передается на Сервер администрирования и регистрируется в базе данных

(см. таблицу ниже).

Таблица 21. Расход трафика

Сценарий	Передача на Сервер администрирования данных при наступлении события "Найден вирус"	Передача на Сервер администрирования данных при наступлении девяти событий "Найден вирус"
Трафик от клиентского устройства к Серверу администрирования, КБ	27,2	100,4
Трафик от Сервера администрирования к клиентскому устройству, КБ	25,8	52,5
Общий трафик (для одного клиентского устройства), КБ	53,0	152,9

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусной программы и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

Расход трафика за сутки

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии "покоя", когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

Таблица 22. Расход трафика

Сценарий	Состояние "покоя" системы администрирования
Трафик от клиентского устройства к Серверу администрирования, КБ	2 162,2
Трафик от Сервера администрирования к клиентскому устройству, КБ	51 000,2
Общий трафик (для одного клиентского устройства), КБ	53 162,4

Подготовка к управлению мобильными устройствами

Этот раздел содержит информацию:

- о сервере мобильных устройств Exchange ActiveSync для управления мобильными устройствами по протоколу Exchange ActiveSync;
- о сервере iOS MDM для управления iOS-устройствами путем установки на них специализированных iOS MDM-профилей;
- об управлении мобильными устройствами с установленным приложением Kaspersky Endpoint Security для Android.

В этом разделе

Сервер мобильных устройств Exchange ActiveSync

Сервер мобильных устройств Exchange ActiveSync® позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync (EAS-устройствами).

В этом разделе

Способы развертывания Сервера мобильных устройств Exchange ActiveSync

Если в организации развернуто несколько серверов Microsoft Exchange с ролью клиентского доступа, объединенных в массив (Client Access Server Array), то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на каждый сервер в массиве. В мастере установки Сервера мобильных устройств Exchange ActiveSync необходимо выбрать **Режим кластера**. В этом случае совокупность экземпляров Сервера мобильных устройств Exchange ActiveSync, установленных на серверы массива, будет называться кластером Серверов мобильных устройств Exchange ActiveSync.

Если в организации не развернут массив серверов Microsoft Exchange с ролью клиентского доступа, то Сервер мобильных устройств Exchange ActiveSync следует устанавливать на сервер Microsoft Exchange, имеющий роль Client Access. При этом в мастере установки Сервера мобильных устройств Exchange

ActiveSync необходимо выбрать **Обычный режим**.

Вместе с Сервером мобильных устройств Exchange ActiveSync на устройство необходимо установить Агент администрирования, с помощью которого осуществляется интеграция Сервера с Kaspersky Security Center.

По умолчанию область сканирования Сервера мобильных устройств Exchange ActiveSync – это текущий домен Active Directory, в котором он установлен. В случае развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2010–2013 имеется возможность расширить область сканирования на весь лес доменов, (см. раздел "Настройка области сканирования" на стр. 703). Запрашиваемая при сканировании информация включает в себя учетные записи пользователей сервера Microsoft Exchange, политики Exchange ActiveSync и мобильные устройства пользователей, подключенные к серверу Microsoft Exchange по протоколу Exchange ActiveSync.

В пределах одного домена недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync, работающих в **Обычном режиме** и управляемых одним и тем же Сервером администрирования.
В пределах одного леса доменов Active Directory также недопустима установка нескольких экземпляров Сервера мобильных устройств Exchange ActiveSync (или нескольких кластеров Сервера мобильных устройств Exchange ActiveSync), работающих в **Обычном режиме**, с расширенной областью сканирования на весь лес доменов и подключенных к одному и тому же Серверу администрирования.

См. также:

Настройка области сканирования 703

Необходимые права для развертывания Сервера мобильных устройств Exchange ActiveSync

Для развертывания Сервера мобильных устройств Exchange ActiveSync на серверах Microsoft Exchange 2010–2013 требуются права доменного администратора и роль Organization Management. Для развертывания Сервера мобильных устройств Exchange ActiveSync на сервере Microsoft Exchange 2007 требуются права доменного администратора и членство в группе безопасности Exchange Organization Administrators.

Учетная запись для работы службы Exchange ActiveSync

В процессе установки Сервера мобильных устройств Exchange ActiveSync в Active Directory автоматически создается учетная запись:

- на сервере Microsoft Exchange 2010–2013 – учетная запись KLMDM4ExchAdmin***** с ролью KLMDM Role Group;
- на сервере Microsoft Exchange 2007 – учетная запись KLMDM4ExchAdmin*****, являющаяся членом группы безопасности KLMDM Secure Group.

Под этой учетной записью работает служба Сервера мобильных устройств Exchange ActiveSync.

Если вы хотите отказаться от автоматического создания учетной записи, то необходимо создать собственную учетную запись, обладающую следующими правами:

- В случае использования сервера Microsoft Exchange 2010–2013 учетная запись должна обладать ролью, для которой разрешено выполнение следующих командлетов:
  - Get-CASMailbox;
  - Set-CASMailbox;
  - Remove-ActiveSyncDevice;
  - Clear-ActiveSyncDevice;
  - Get-ActiveSyncDeviceStatistics;
  - Get-AcceptedDomain;
  - Set-AdServerSettings;
  - Get-ActiveSyncMailboxPolicy;
  - New-ActiveSyncMailboxPolicy;
  - Set-ActiveSyncMailboxPolicy;
  - Remove-ActiveSyncMailboxPolicy.
- В случае использования сервера Microsoft Exchange 2007, для учетной записи должны быть назначены права доступа к объектам Active Directory (см. таблицу ниже).

Таблица 23. Права доступа к объектам Active Directory

Доступ	Объект	Командлет
Полный	Ветка "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`
Чтение	Ветка "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`

Доступ	Объект	Командлет
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	`Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Имя домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Расширенное право ms-Exch-Store-Active	Хранилища почтовых ящиков Exchange-сервера, ветка "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>"	`Get-MailboxDatabase | Add-ADPermission -User <Имя пользователя или группы> -ExtendedRights ms-Exch-Store-Admin`

Сервер iOS MDM

Сервер iOS MDM позволяет осуществлять управление iOS-устройствами путем установки на них специализированных iOS MDM-профилей. Поддерживаются следующие функции:

- блокирование устройства;
- сброс пароля;
- удаление данных устройства;
- установка или удаление приложений;
- применение iOS MDM-профиля с дополнительными параметрами (такими как параметры VPN, почты, Wi-Fi, камеры, сертификаты, и так далее).

Сервер iOS MDM представляет собой веб-сервис, который принимает входящие соединения от мобильных устройств на свой TLS-порт (по умолчанию порт 443) и управляется со стороны Kaspersky Security Center с помощью Агента администрирования. Агент администрирования устанавливается локально на устройстве с развернутым Сервером iOS MDM.

В процессе развертывания Сервера iOS MDM администратору необходимо выполнить следующие действия:

- обеспечить Агенту администрирования доступ к Серверу администрирования;
- обеспечить мобильным устройствам доступ к TCP-порту Сервера iOS MDM.

В этом разделе рассмотрены две типовые конфигурации Сервера iOS MDM.

В этом разделе

Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне

Сервер iOS MDM располагается в демилитаризованной зоне сети организации с доступом в интернет. Особенностью данного подхода является отсутствие проблем с доступностью веб-сервиса iOS MDM из интернета со стороны устройств.

Так как для управления Сервером iOS MDM требуется локально установленный Агент администрирования, необходимо обеспечить взаимодействие этого Агента администрирования с Сервером администрирования. Это можно сделать следующими способами:

- Поместить Сервер администрирования в демилитаризованную зону.
- Использовать шлюз соединений (см. раздел "Доступ из интернета:Использовать в качестве шлюза соединений в демилитаризованной зоне" на стр. 85):
  a. На устройстве с развернутым Сервером iOS MDM подключить Агент администрирования к Серверу администрирования через шлюз соединений.
  b. На устройстве с развернутым Сервером iOS MDM назначить Агент администрирования шлюзом соединений.

См. также:

Типовая конфигурация: Сервер iOS MDM в локальной сети организации

Сервер iOS MDM располагается во внутренней сети организации. Порт 443 (порт по умолчанию) должен быть доступным извне, например, посредством публикации веб-сервиса iOS MDM на Microsoft Forefront® Threat Management Gateway (далее TMG) (см. раздел "Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)" на стр. 171).

В любой типовой конфигурации потребуется обеспечить доступность для Сервера iOS MDM веб-сервисов Apple (диапазон адресов 17.0.0.0/8) по порту TCP 2195. Этот порт используется для оповещения устройств о новых командах через специализированный сервис APNs (см. раздел "Настройка доступа к сервису Apple Push Notification" на стр. 167).

Управление мобильными устройствами с установленным Kaspersky Endpoint Security для Android

Управление мобильными устройствами с установленным приложением Kaspersky Endpoint Security для

Android™ (далее KES-устройства) осуществляется с помощью Сервера администрирования. В программе Kaspersky Security Center 10 Service Pack 1 и выше поддерживаются следующие возможности по управлению KES-устройствами:

- работа с мобильными устройствами как с клиентскими устройствами:
  - членство в группах администрирования;
  - статусы, события, отчеты и прочее;
  - изменение локальных параметров и назначение политик для приложения Kaspersky Endpoint Security для Android;
- централизованная отправка команд;
- удаленная установка пакетов мобильных приложений.

Обслуживание KES-устройств осуществляется Сервером администрирования по протоколу TLS, порт TCP 13292.

См. также:

Предоставление доступа к Серверу администрирования из интернета 84

Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций, а также ограничения на подключение управляемых устройств к Серверу администрирования.

В этом разделе

Ограничения подключений к Серверу администрирования

Сервер администрирования поддерживает управление до 100 000 устройств без потери производительности.

Ограничения на подключения к Серверу администрирования без потери производительности:

- Один Сервер администрирования может поддерживать до 500 виртуальных Серверов

администрирования.

- Главный Сервер администрирования поддерживает одновременно не более 1000 сессий.
- Виртуальные Серверы администрирования поддерживают одновременно не более 1000 сессий.

См. также:

Результаты тестов производительности Сервера администрирования 105

Результаты тестов производительности Сервера администрирования

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные промежутки времени. Эта информация может быть использована для выбора оптимальных схем развертывания антивирусной защиты в компьютерных сетях.

Для тестирования использовались устройства со следующими аппаратными конфигурациями (см. таблицы ниже):

Таблица 24. Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel Xeon CPU E5506, тактовая частота 2,13 ГГц, 1 сокет, 8 ядер
ОЗУ	4 МБ
Жесткий диск	IBM ServeRAID M5015 SCSI Disk Device, 928 ГБ
Операционная система	Microsoft Windows Server 2008 R2 Standard, Service Pack 1, 6.1.7601
Сеть.	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Таблица 25. Аппаратная конфигурация устройства с SQL Server

Параметр	Значение
Процессор	Intel Xeon CPU E5630, тактовая частота 2,53 ГГц, 1 сокет, 8 ядер, 16 логических процессоров
ОЗУ	26 ГБ
Жесткий диск	IBM ServeRAID M5014 SCSI Disk Device, 929 ГБ
Операционная система	Microsoft Windows Server 2012 R2 Standard, 6.3.9600
Сеть.	Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

Сервер администрирования поддерживал создание 500 виртуальных Серверов администрирования.

Период синхронизации составлял по 15 минут на каждые 10 000 управляемых устройств (см. таблицу ниже).

Таблица 26. Обобщенные результаты нагрузочного тестирования Сервера администрирования

Период синхронизации, мин.	Количество управляемых устройств
15	10 000
30	20 000

Период синхронизации, мин.	Количество управляемых устройств
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Результаты тестирования производительности прокси-сервера KSN

Если ваша корпоративная сеть включает в себя большое количество клиентских устройств, и они используют Сервер администрирования в качестве прокси-сервера KSN, Сервер администрирования должен удовлетворять определенным аппаратным требованиям, чтобы обрабатывать запросы с клиентских устройств. Вы можете использовать результаты тестирования ниже для оценки загрузки Сервера администрирования в вашей сети и планирования аппаратных ресурсов, для обеспечения нормальной работы службы прокси-сервера KSN.

В таблице ниже приведена конфигурация аппаратного обеспечения Сервера администрирования, которая была использована для тестирования.

Таблица 27. Аппаратная конфигурация Сервера администрирования

Параметр	Значение
Процессор	Intel(R) Xeon(R) CPU E5540, тактовая частота 2,53 ГГц, 2 сокета, 8 ядер, гиперпотоковые возможности процессора выключены
ОЗУ	18 ГБ
Операционная система	Microsoft Windows Server 2012 R2 Standard

В таблице ниже приведены результаты тестирования.

Таблица 28. Обобщенные результаты тестирования производительности прокси-сервера KSN

Параметр	Значение
Максимальное количество обработанных запросов в секунду	около 15 000
Максимальное использование процессора	60%

Скорость заполнения базы данных событиями Kaspersky Endpoint Security

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования.

В базу данных поступает (Ne*Nh) событий в день (см. таблицу ниже). Здесь Nh – количество клиентских устройств, на которых установлены управляемые программы. Ne – количество событий в день, информацию о которых передает с клиентского устройства установленная на нем управляемая программа Kaspersky Endpoint Security для Windows. По умолчанию Kaspersky Endpoint Security для Windows (версии 10 и 11) при штатной работе передает в базу данных около 20 событий в день. Максимальное количество

событий, которое может обработать Kaspersky Security Center, составляет 2 000 000 событий в день.

Таблица 29. Скорость заполнения событиями базы данных (при штатной работе)

Количество устройств, на которых установлена программа Kaspersky Endpoint Security	Количество событий, передаваемое в базу данных в день
100	до 2 000
1 000	до 20 000
10 000	до 200 000
100 000	до 2 000 000

Максимальное количество событий, хранящихся в базе данных, определяется в разделе **Хранилище событий** окна свойств Сервера администрирования. По умолчанию в базе данных хранится не более 400 000 событий.

Развертывание Агента администрирования и программы безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); и обнаружение уязвимостей программ сторонних производителей (при использовании Системного администрирования).

В этом разделе

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная инсталляция приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства. Подробные сведения об установке программ на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки приложений.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows или автоматизированно, с помощью соответствующего параметра в задаче удаленной установки приложений Kaspersky Security Center.
- Принудительно с помощью соответствующих параметров в задаче удаленной установки программ Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные

Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных программ с настроенными параметрами.

- Вручную, запуская инсталляторы программ на устройствах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых устройствах следует осуществлять имеющимися сторонними средствами. Обновлять Агент администрирования до новой версии, а также устанавливать другие приложения "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания программ в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- Настройка сети организации (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 79).
- общего количества устройств;
- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности использование UAC и режима Simple File Sharing).

В этом разделе

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети программ "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки программы. При установке Агента администрирования требуется задать по крайней мере адрес для подключения к Серверу администрирования, а возможно, и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для неинтерактивной "тихой" установки программ на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для неинтерактивной установки на выбранные устройства в сети.

Инсталляционные пакеты

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в формате Microsoft Windows Installer (MSI) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. раздел "Задание папки общего доступа" на стр. 183).

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

О том, как именно можно воспользоваться этим способом настройки параметров для приложений "Лаборатории Касперского" перед их развертыванием сторонними средствами, см. в разделе "Развертывание с помощью механизма групповых политик Microsoft Windows" (на стр. 115).

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и программы безопасности для платформы Microsoft Windows.

Несмотря на то, что ключ для лицензии на приложение можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за широкой доступности инсталляционных пакетов на чтение. Следует использовать автоматически распространяемые ключи или задачи установки ключей.

Свойства MSI и файлы трансформации

Другим способом настроить параметры инсталляции на платформе Windows является задание свойств MSI и файлов трансформации. Этот способ может быть использован в следующих случаях:

- при установке через групповые политики Windows при помощи штатных средств Microsoft или иных сторонних инструментов для работы с групповыми политиками Windows;
- при установке с помощью сторонних средств, ориентированных на работу с инсталляторами в формате Microsoft Installer (см. раздел "Настройка параметров инсталляторов" на стр. 124).

Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

См. также:

Задание папки общего доступа 183

Настройка параметров инсталляторов 124

Общие сведения о задачах удаленной установки приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска, установка с помощью групповых политик Microsoft Windows). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и / или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание захватом и копированием образа жесткого диска устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа жесткого диска устройства.

Развертывание путем захвата и копирования образа жесткого диска нужно выполнять следующим образом:

1. Создать "эталонное" устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и программу безопасности.
2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center.

   Для захвата и установки образов диска можно воспользоваться как имеющимися в организации сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии на Системное администрирование) Kaspersky Security Center (см. раздел "Установка образов операционных систем" на стр. 90).

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на устройство из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемое устройство. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать устройства, созданные путем копирования одного и того же образа.
При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- Рекомендуемый метод. Во время установки Агента администрирования на эталонное устройство снять флажок **Запустить программу в процессе установки**, на соответствующем шаге мастера установки, и захватить образ устройства до первого старта службы Агента администрирования (так как уникальная информация, идентифицирующая устройство, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.
- На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.
- Обеспечить запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на устройствах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.

Если копирование образа жесткого диска было выполнено неправильно, см. раздел "Неверно выполнено копирование образа жесткого диска" (на стр. 832).

Можно применять альтернативный вариант развертывания Агента администрирования на новые устройства с использованием образов операционной системы:

- Захваченный образ не содержит установленный Агент администрирования.
- В список исполняемых файлов, запускаемых по завершении развертывания образа на устройствах, добавлен автономный пакет Агента администрирования, расположенный в папке общего доступа Kaspersky Security Center.

Этот вариант развертывания дает большую гибкость: можно использовать один образ операционной системы совместно с различными вариантами установки Агента и / или программы безопасности, включая правила перемещения устройства, связанные с автономным пакетом. При этом несколько усложняется процесс развертывания, требуется обеспечить доступ к сетевой папке с автономными пакетами с устройства (см. раздел "Установка образов операционных систем" на стр. 90).

Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть данного способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.
- Область действия установки задается привязкой к организационному подразделению и / или к группе безопасности, в которую входят устройства.
- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему. Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до

перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows.

Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center

Самым простым способом инсталляции приложений при помощи групповых политик Microsoft Windows является установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит устройства, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет актуализироваться при каждом запуске задачи в соответствии с набором устройств на момент запуска.

Для обеспечения работоспособности данной функции следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, установка флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на устройстве. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования). Не все приложения могут быть установлены с помощью групповых политик Microsoft Windows. О такой возможности вы можете узнать, обратившись к информации о способах установки приложения.

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством устройств и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище (см. раздел "Задание папки общего доступа" на стр. 183).

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться устройства по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание устройств для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором устройств задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

Самостоятельная установка приложений с помощью политик Microsoft Windows

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на msi-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.
- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается msi-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации.
- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс организации. Объект групповой политики ссылается msi-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MSI (см. раздел "Настройка параметров инсталляторов" на стр. 124).

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

В случае если требуется начать развертывание Агентов администрирования или других необходимых приложений немедленно, без ожидания очередного входа устройств в домен, или же при наличии устройств, не являющихся членами домена Active Directory, можно использовать принудительную (форсированную) установку выбранных инсталляционных пакетов при помощи задачи удаленной установки приложений Kaspersky Security Center.

Устройства при этом могут задаваться явно (списком) либо выбором группы администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Данный способ установки осуществляется путем копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. При этом должны

выполняться следующие условия:

- Устройства должны быть доступны для подключения либо со стороны Сервера администрирования, либо со стороны точки распространения.
- В сети должно корректно работать разрешение имен для устройств.
- На управляемых устройствах не должны быть отключены административные ресурсы общего доступа admin$.
- На устройствах должна быть запущена системная служба Server (по умолчанию данная служба запущена).
- На устройствах должны быть открыты следующие порты для удаленного доступа к устройствам средствами Windows: TCP 139, TCP 445, UDP 137, UDP 138.
- На устройствах должен быть выключен режим Simple File Sharing.
- На устройствах модель совместного доступа и безопасности для локальных учетных записей должна находиться в состоянии *Обычная – локальные пользователи удостоверяются как они сами* (Classic – local users authenticate as themselves), и ни в коем случае не в состоянии *Гостевая – локальные пользователи удостоверяются как гости* (Guest only – local users authenticate as Guest).
- Устройства должны быть членами домена, либо на устройствах должны быть заблаговременно созданы унифицированные учетные записи с административными правами.

Устройства, расположенные в рабочих группах, могут быть приведены в соответствие указанным выше требованиям при помощи утилиты riprep.exe, которая описана на портале Службы технической поддержки "Лаборатории Касперского".

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Можно использовать упрощенный способ создания задач принудительной установки приложений – автоматическую установку. Для этого в свойствах группы администрирования нужно выбрать в списке инсталляционных пакетов те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне.

Для работоспособности принудительной установки необходимо обеспечить наличие точек распространения в каждой такой изолированной сети.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети. Однако следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Поэтому нужно выбирать в качестве точек распространения мощные устройства с высокопроизводительными накопителями. Также необходимо, чтобы объем свободного места в разделе с папкой *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* многократно превосходил суммарный объем дистрибутивов устанавливаемых приложений (см. раздел "Требования для точки распространения" на стр. 842).

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный пакет установки размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом "тихой" установки "-s"). Автономный пакет установки можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого приложения (например, программы безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в "тихом" режиме (при запуске с ключом "-s"). "Тихий" режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в "тихом" режиме определяется кодом возврата процесса.

Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них

инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в "тихом" режиме с параметрами, заданными при настройке инсталляционного пакета.

При запуске setup.exe из корня инсталляционного пакета расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается флажком **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений (см. раздел "Общие сведения о задачах удаленной установки приложений Kaspersky Security Center" на стр. 113).

Если флажок установлен, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене точки распространения (см. разделы "О точках распространения" на стр. 86 и "Построение структуры групп администрирования и назначение точек распространения" (см. раздел "Настройка точек распространения и шлюзов соединений" на стр. 534)). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания программ.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную нельзя. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp.

Удалять файлы из папки $FTClTmp вручную нельзя. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, нельзя вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно выбрать вариант действия при необходимости перезагрузки:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.
- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
- **Запрашивать у пользователя**. На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения

пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

Целесообразность обновления баз в инсталляционном пакете программы безопасности

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом программы безопасности. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания безопасности на устройствах.

Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную kud-файл, сформированный Kaspersky Security Center в папке созданного инсталляционного пакета.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

Пример:

[SetupProcessResult]

Wait=0

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

Пример:

[SetupProcessResult]

WaitJob=0

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, нужно перечислить успешные коды возврата в секции [SetupProcessResult_SuccessCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0=

3010=

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

Пример:

[SetupProcessResult_SuccessCodes]

0 = установка завершена успешно

3010=A reboot is required to complete the installation

[SetupProcessResult_ErrorCodes]

1602=Installation cancelled by the user

1603 = критическая ошибка при установке

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды

возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

Пример:

[SetupProcessResult_NeedReboot]

3010=

Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах программы безопасности и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования (см. раздел "Цветовые индикаторы в Консоли администрирования" на стр. 460). Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и программами безопасности. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки, здесь отображается количество ошибок. Просмотреть детальную информацию об ошибке можно по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на закладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и программой безопасности.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки. В контекстном меню задачи выберите **Результаты**. В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записывается в Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в узле Сервера администрирования на закладке **События**.

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в "тихом" режиме.

В этом разделе

Общая информация

Инсталляторы компонентов Kaspersky Security Center 11 – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является msi-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и msi-пакет, и используется автоматически при установке в тихом режиме. Тихий режим установки включается ключом командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров установочных пакетов в Консоли администрирования.

Установка в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент

администрирования, используя групповые политики. Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства DONT_USE_ANSWER_FILE=1. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Пример:

msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

Пример:

msiexec /I "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst

В одной команде можно указать более одного файла трансформации.

Частичная настройка параметров установки через setup.exe

Запуская установку программ через setup.exe, можно передавать в msi-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:

/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"

Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются необязательными, кроме EULA и PRIVACYPOLICY.

Таблица 30. Параметры установки Сервера администрирования в неинтерактивном режиме

Свойство MSI	Описание	Возможные значения
EULA	Согласие с условиями и лицензии (обязательный параметр).	• 1 – Я принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).

Свойство MSI	Описание	Возможные значения
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности (обязательный параметр).	• 1 – Я принимаю условия Политики конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Стандартная. • Выборочная.
INSTALLDIR	Папка установки программы.	Строковое значение.
ADDLOCAL	Список компонентов для установки (через запятую).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети.	• NRT_1_100 – от 100 до 100 устройств. • NRT_100_1000 – от 100 до 1 000 устройств. • NRT_GREATER_1000 – более 1000 устройств.

Свойство MSI	Описание	Возможные значения
SRV_ACCOUNT_TYPE	Способ задания пользователя для работы службы Сервера администрирования.	• SrvAccountDefault – учетная запись пользователя будет создана автоматически. • SrvAccountUser – учетная запись пользователя задана вручную.
SERVERACCOUNTNAME	Имя пользователя для службы.	Строковое значение.
SERVERACCOUNTPWD	Пароль пользователя для службы.	Строковое значение.
DBTYPE	Тип базы данных.	• MySQL. • MSSQL.
MYSQLSERVERNAME	Полное имя mysql-сервера.	Строковое значение.
MYSQLSERVERPORT	Номер порта для подключения к mysql-серверу.	Числовое значение.
MYSQLDBNAME	Имя базы данных mysql-сервера.	Строковое значение.

Свойство MSI	Описание	Возможные значения
MYSQLACCOUNTNAME	Имя пользователя для подключения к базе mysql-сервера.	Строковое значение.
MYSQLACCOUNTPWD	Пароль пользователя для подключения к базе mysql-сервера.	Строковое значение.
MSSQLCONNECTIONTYPE	Тип использования базы данных MSSQL.	• InstallMSSEE – инсталлировать из пакета; • ChooseExisting –использовать установленный сервер.
MSSQLSERVERNAME	Полное имя экземпляра SQL Server.	Строковое значение.
MSSQLDBNAME	Имя базы данных SQL Server.	Строковое значение.
MSSQLAUTHTYPE	Способ аутентификации при подключении к SQL Server.	• Windows. • SQLServer.

Свойство MSI	Описание	Возможные значения
MSSQLACCOUNTNAME	Имя пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.
MSSQLACCOUNTPWD	Пароль пользователя для подключения к SQL Server в режиме SQLServer.	Строковое значение.

CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа; в этом случае должны быть заданы свойства:
		  • SHARELOCALPATH – путь к локальной папке.
		  • SHAREFOLDERNAME – сетевое имя папки.
		• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа.	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.

Свойство MSI	Описание	Возможные значения
SERVERSSLPORT	Номер порта для установки SSL-соединения с Сервером администрирования.	Числовое значение.
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
SERVERCERT2048BITS	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит. • Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 1024 бит.
MOBILESERVERADDRESS	Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport.	Строковое значение.

См. также:

Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме EULA и SERVERADDRESS.

Таблица 31. Параметры установки Агента администрирования в неинтерактивном режиме

Свойство MSI	Описание	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – Я принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Читать параметры установки из файла ответов.	• 1 – читать; • другое значение или не задано – не читать.
INSTALLDIR	Путь к папке установки Агента администрирования.	Строковое значение.
SERVERADDRESS	Адрес Сервера администрирования (обязательный параметр).	Строковое значение.
SERVERPORT	Номер порта подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.
USESSL	Использовать ли SSL-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	• 1 – открывать; • другое значение или не задано – не открывать.

Свойство MSI	Описание	Возможные значения
UDPPORT	Номер UDP-порта.	Числовое значение.
USEPROXY	Использовать ли прокси-сервер.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYADDRESS	Адрес прокси-сервера.	Строковое значение.
PROXYPORT	Номер порта для подключения к прокси-серверу.	Числовое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу. Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE.
CERTFILE	Путь к файлу сертификата.	Строковое значение.
VMVDI	Включить динамический режим для VDI.	• 1 – включать; • другое значение или не задано – не включать.

Свойство MSI	Описание	Возможные значения
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки.	• 1 – запускать; • другое значение или не задано – не запускать.
NAGENTTAGS	Тег для Агента администрирования (будет иметь приоритет над тегом, указанным в файле ответов).	• Строковое значение.

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Поддерживается установка Агента администрирования и программы безопасности на каждую виртуальную машину и защита виртуальных машин на уровне гипервизора. В первом случае для защиты виртуальных машин может использоваться как обычная программа безопасности, так и Kaspersky Security для виртуальных сред / Легкий агент для защиты виртуальных машин. Во втором случае для защиты виртуальных машин используется Kaspersky Security для виртуальных сред / Защита без агента.

Начиная с версии 10 Maintenance Release 1, Kaspersky Security Center поддерживает откат виртуальных машин в предыдущее состояние (см. раздел "Поддержка отката файловой системы для устройств с Агентом администрирования" на стр. 136).

В этом разделе

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, целесообразно выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) установить флажок **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера установить флажок **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Установка флажков изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины (только для Windows). Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно установить флажок **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. 143);
- в случае интерактивной установки – в окне мастера установки Агента администрирования.

Флажок **Включить динамический режим для VDI** не следует устанавливать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** установить флажок **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска (см. раздел "Развертывание захватом и копированием образа жесткого диска устройства" на стр. 113).

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе "Развертывание захватом и копированием жесткого диска устройства", необязательно:

- При установке Агента администрирования был установлен флажок **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенной программой. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой

системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center 11 поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 561).

Локальная установка программ

В этом разделе описана процедура установки программ, которые могут быть установлены на устройства только локально.

Для проведения локальной установки программ на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► *Чтобы установить программы локально на выбранное клиентское устройство, выполните следующие действия:*

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.
2. Установите на устройство необходимые программы согласно описаниям, изложенным в Руководствах к этим программам.
3. Установите на рабочее место администратора плагин управления для каждой из установленных программ.

Kaspersky Security Center также поддерживает возможность локальной установки программ с помощью автономного пакета установки. Kaspersky Security Center не поддерживает установку всех программ "Лаборатории Касперского" (см. раздел "Список поддерживаемых программ "Лаборатории Касперского" на стр. 30).

Вы можете получить сведения о последних версиях программ на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center 11, в разделе Общая информация (http://support.kaspersky.ru/14757) .

В этом разделе

Локальная установка Агента администрирования

► *Чтобы установить Агент администрирования на устройство локально, выполните следующие*

действия:

1. На устройстве запустите файл setup.exe из дистрибутива, полученного через интернет.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить только Агент администрирования Kaspersky Security Center 11** запустите мастер установки Агента администрирования. Следуйте далее указаниям мастера.

   Во время работы мастера установки вы можете настроить дополнительные параметры Агента администрирования (см. ниже).

3. Чтобы использовать устройство в качестве шлюза соединений для выбранной группы администрирования, в окне **Шлюз соединений** мастера установки выберите вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.

4. Чтобы настроить Агент администрирования при установке на виртуальную машину, выполните следующие действия:

   a. Если вы планируете создать динамически виртуальные машины из образов виртуальных машин, включите динамический режим Агента администрирования для Virtual Desktop Infrastructure (VDI). Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Включить динамический режим для VDI**.

      Пропустите этот шаг, если вы не планируете создавать динамически виртуальные машины из образов виртуальных машин.

      Использование динамического режима для VDI доступно только для устройств под управлением Windows.

   b. Оптимизируйте работу Агента администрирования для виртуальной инфраструктуры. Для этого в окне мастера установки **Дополнительные параметры** установите флажок **Оптимизировать параметры Агента администрирования Kaspersky Security Center для виртуальной инфраструктуры**.

      В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

      - о реестре оборудования;
      - о программах, установленных на устройстве;
      - об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
      - об уязвимостях программного обеспечения, обнаруженных на локальном клиентском устройстве.

      В дальнейшем вы сможете включить передачу этой информации в свойствах Агента администрирования или в параметрах политики Агента администрирования.

По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просмотреть свойства службы Агента администрирования Kaspersky Security Center, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером \ Службы.

См. также:

Поддержка динамических виртуальных машин.....135

Установка Агента администрирования в неинтерактивном режиме

Агент администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки. Для неинтерактивной установки используется установочный пакет (.msi) Агента администрирования. Файл .msi расположен в дистрибутиве программы Kaspersky Security Center в папке Packages\NetAgent\exec.

► *Чтобы установить Агент администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PROP1=PROP1VAL PROP2=PROP2VAL`).

В список параметров вы должны включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Установка Агента администрирования в неинтерактивном режиме требует принятия Лицензионного соглашения. Просмотреть Лицензионное соглашение Агента администрирования можно в комплекте поставки Агента администрирования или на веб-сайте Службы технической поддержки "Лаборатории Касперского". Пожалуйста, внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми пунктами Лицензионного соглашения, включите параметр `EULA=1` в список параметров команды. Использование параметра `EULA=1` означает, что вы принимаете условия Лицензионного соглашения.

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в неинтерактивном режиме, приведены в разделе Параметры установки Агента администрирования на стр. 132.

См. также:

Параметры установки Агента администрирования 132

Параметры установки Сервера администрирования 126

Локальная установка плагина управления программой

► *Чтобы установить плагин управления программой,*

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл klcfginst.exe, входящий в дистрибутивный пакет этой программы.

Файл klcfginst.exe входит в состав всех программ, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

Установка программ в неинтерактивном режиме

► *Чтобы провести установку программы в неинтерактивном режиме, выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Security Center.
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужной программы или сформируйте для этой программы новый инсталляционный пакет.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:
   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.
   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Выключено** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности**).

4. В зависимости от выбранной программы выполните следующие действия:

   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.
   - Для остальных программ "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

   Запуск исполняемого файла с ключами `EULA=1` и `PRIVACYPOLICY=1` означает, что вы принимаете положения Лицензионного соглашения и Политики конфиденциальности соответственно. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы или обновления предыдущей версии программы.

Установка программ с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные пакеты установки программ. Автономный пакет установки представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center.

► *Чтобы установить программу с помощью автономного пакета установки, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области выберите инсталляционный пакет нужной программы.
4. Запустите процесс создания автономного пакета установки одним из следующих способов:

   - в контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**;
   - по ссылке **Создать автономный пакет установки** в блоке работы с инсталляционным пакетом.

   В результате запускается мастер создания автономного пакета установки. Следуйте далее

указаниям мастера.

На завершающем шаге мастера выберите способ передачи автономного пакета установки на клиентское устройство.

5. Передайте автономный пакет установки программы на клиентское устройство.
6. Запустите автономный пакет установки на клиентском устройстве.

В результате программа будет установлена на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный пакет установки автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных пакетов установки. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных пакетов установки используется порт 8060.

Параметры инсталляционного пакета Агента администрирования

► *Чтобы настроить параметры инсталляционного пакета Агента администрирования, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета Агента администрирования.

Общие

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию программы, для которой сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дату создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

Параметры

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки. Параметры этого раздела доступны только для устройств под управлением Windows.

В блоке параметров **Папка установки** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования:

- **Устанавливать в папку по умолчанию**

  Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет создана автоматически.

  По умолчанию этот вариант выбран.

- **Устанавливать в заданную папку**

  Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

  Если флажок установлен, при нажатии на кнопку **Изменить** можно ввести пароль для удаления программы (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

  По умолчанию флажок снят.

- **Состояние**

  Статус пароля: **Пароль задан** или **Пароль не задан**.

  По умолчанию пароль не установлен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  После того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена.

  По умолчанию параметр выключен.

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**

  Если флажок установлен, то загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера мобильных устройств Exchange ActiveSync и Сервера iOS MDM будут устанавливаться автоматически (автоматическая установка доступна для Агента администрирования начиная с версии Kaspersky Security Center 10 Service Pack 2).

  Если флажок снят, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

  По умолчанию флажок установлен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования.

- **Адрес Сервера**

  Адрес устройства, на котором установлен Сервер администрирования.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Номер SSL-порта**

  Номер порта, по которому будет выполняться подключение с использованием протокола SSL.

- **Использовать сертификат Сервера**

  Если флажок установлен, для аутентификации доступа Агента администрирования к Серверу администрирования будет использоваться файл сертификата, который можно указать при нажатии на кнопку **Обзор**.

  Если флажок не установлен, файл сертификата будет получен с Сервера администрирования при первом подключении Агента администрирования по адресу, указанному в поле **Адрес сервера**.

  Не рекомендуется снимать флажок, так как автоматическое получение сертификата Сервера администрирования Агентом администрирования при подключении к Серверу является небезопасным.

  По умолчанию флажок установлен.

- **Использовать SSL-соединение**

  Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию флажок снят.

- **Использовать UDP-порт**

  Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт.

  По умолчанию флажок установлен.

- **Номер UDP-порта**

  В поле можно указать номер порта подключения Агента администрирования к Серверу администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если флажок установлен, после установки Агента администрирования на клиентском устройстве в список исключений брандмауэра Microsoft Windows будет

добавлен UDP-порт. Этот UDP-порт требуется для корректной работы Агента администрирования.

По умолчанию флажок установлен.

Дополнительно

В разделе **Дополнительно** можно настроить параметры использования шлюза соединений:

- **Использовать в качестве шлюза соединений в демилитаризованной зоне**

  Если флажок установлен, Агент администрирования будет использоваться в качестве шлюза соединений в демилитаризованной зоне.

  По умолчанию флажок снят.

- **Подключаться к Серверу администрирования через шлюз соединений**

  Если флажок установлен, Агент администрирования будет подключаться к Серверу администрирования через шлюз соединений.

  По умолчанию флажок снят.

- **Адрес шлюза соединений.**

  В поле ввода можно указать адрес устройства, который будет использоваться в качестве шлюза соединений.

  Поле недоступно, когда снят флажок **Подключаться к Серверу администрирования через шлюз соединений**.

- **Включить динамический режим для VDI**

  Если флажок установлен, для Агента администрирования, установленного на виртуальной машине, будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

  По умолчанию флажок снят.

- **Оптимизировать параметры для VDI**

Если флажок установлен, в параметрах Агента администрирования выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

  По умолчанию флажок снят.

Дополнительные компоненты

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

Теги

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета (см. раздел "Работа с ревизиями объектов" на стр. 654). Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Параметры инсталляционного пакета Агента администрирования доступны для конкретной операционной системы, которые приведены в таблице ниже.

Таблица 32. Параметры инсталляционного пакета Агента администрирования

Раздел свойств	Windows.	Mac	Linux
Общие	+	+	+
Параметры	+	Нет	Нет
Подключение	+	+ * кроме флажков: **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** **Использовать только автоматическое определение прокси-сервера**	+ * кроме флажков: **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** **Использовать только автоматическое определение прокси-сервера**
Дополнительно	+	+	+
Дополнительные компоненты	+	+	+

Раздел свойств	Windows.	Mac	Linux
Теги	+	+ * кроме правил автоматического назначения тегов	+ * кроме правил автоматического назначения тегов
История ревизий	+	+	+

Развертывание систем управления мобильными устройствами

В этом разделе описано развертывание систем управления мобильных устройств по протоколам Exchange ActiveSync, iOS MDM и Kaspersky Endpoint Security.

В этом разделе

Развертывание системы управления по протоколу Exchange ActiveSync

Kaspersky Security Center позволяет управлять мобильными устройствами, которые подключаются к Серверу администрирования по протоколу Exchange ActiveSync. Мобильными устройствами Exchange ActiveSync (EAS-устройствами) называются мобильные устройства, подключенные к Серверу мобильных устройств Exchange ActiveSync и находящиеся под управлением Сервера администрирования.

Протокол Exchange ActiveSync поддерживает следующие операционные системы:

- Windows Phone® 8;
- Windows Phone 8.1;
- Windows 10 Mobile;
- Android;
- iOS.

Набор параметров управления устройством Exchange ActiveSync зависит от операционной системы, под управлением которой находится мобильное устройство. С особенностями поддержки протокола Exchange ActiveSync для конкретной операционной системы можно ознакомиться в документации для этой операционной системы.

Развертывание системы управления мобильными устройствами по протоколу Exchange ActiveSync выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер мобильных устройств

Exchange ActiveSync (см. раздел "Установка Сервера мобильных устройств Exchange ActiveSync" на стр. 150).

2. Администратор создает в Консоли администрирования профиль (профили) управления EAS-устройствами и добавляет профиль к почтовым ящикам пользователей Exchange ActiveSync.

   Профиль управления мобильными устройствами Exchange ActiveSync – это политика ActiveSync, которая используется на сервере Microsoft Exchange для управления мобильными устройствами Exchange ActiveSync. Почтовому ящику Microsoft Exchange может быть назначен только один профиль управления EAS-устройствами (см. раздел "Управление мобильными устройствами Exchange ActiveSync" на стр. 699).

   Пользователи мобильных EAS-устройств подключаются к своим почтовым ящикам Exchange. Профиль управления накладывает ограничения на мобильные устройства (см. раздел "Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync" на стр. 152).

В этом разделе

Установка Сервера мобильных устройств Exchange ActiveSync

Сервер мобильных устройств Exchange ActiveSync устанавливается на клиентское устройство с установленным сервером Microsoft Exchange. Рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync на сервер Microsoft Exchange с ролью Client Access. Если в одном домене несколько серверов Microsoft Exchange с ролью Client Access объединены в массив (Client Access Array), то рекомендуется устанавливать Сервер мобильных устройств Exchange ActiveSync в режиме кластера на каждый сервер Microsoft Exchange в массиве.

► *Чтобы установить Сервер мобильных устройств Exchange ActiveSync на локальном устройстве, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить Сервер мобильных устройств Exchange ActiveSync** запустите мастер установки Сервера мобильных устройств Exchange ActiveSync.
3. В окне **Настройка установки** выберите тип установки Сервера мобильных устройств Exchange

ActiveSync:

- Если вы хотите установить Сервер мобильных устройств Exchange ActiveSync с использованием параметров по умолчанию, выберите вариант **Стандартная установка** и нажмите на кнопку **Далее**.
- Если вы хотите задать вручную значения параметров установки Сервера мобильных устройств Exchange ActiveSync, выберите вариант **Расширенная установка** и нажмите на кнопку **Далее**. Затем выполните следующие действия:

  a. В окне **Папка назначения** выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

  b. В окне **Режим установки** выберите режим установки Сервера мобильных устройств Exchange ActiveSync: обычный режим или режим кластера.

  c. В окне **Выбор учетной записи** выберите учетную запись, которая будет использоваться для управления мобильными устройствами:

  - **Создать учетную запись и ролевую группу автоматически**. Учетная запись будет создана автоматически.
  - **Задать учетную запись**. Учетную запись следует выбрать вручную. Нажмите на кнопку **Обзор**, чтобы выбрать пользователя, учетная запись которого будет использоваться, и укажите пароль. Выбранный пользователь должен входить в группу с правами на управление мобильными устройствами через ActiveSync.

  d. В окне **Настройка IIS** разрешите или запретите автоматическую настройку параметров веб-сервера Internet Information Services (IIS).

  > Если вы запретили автоматическую настройку параметров IIS, включите вручную механизм аутентификации "Windows authentication" в параметрах IIS для виртуальной директории PowerShell. Если механизм аутентификации "Windows authentication" не будет включен, установленный Сервер мобильных устройств Exchange ActiveSync будет неработоспособен. Информацию о работе с параметрами IIS можно прочитать в документации для этого веб-сервера.

  e. Нажмите **Далее**.

4. В открывшемся окне проверьте значения параметров установки Сервера мобильных устройств Exchange ActiveSync и нажмите на кнопку **Установить**.

В результате работы мастера будет выполнена установка Сервера мобильных устройств Exchange ActiveSync на локальное устройство. Сервер мобильных устройств Exchange ActiveSync будет отображаться в папке **Управление мобильными устройствами** дерева консоли.

Подключение мобильных устройств к Серверу мобильных устройств Exchange ActiveSync

Перед подключением мобильных устройств должен быть настроен Microsoft Exchange Server для возможности соединения устройств по протоколу ActiveSync.

Чтобы подключить мобильное устройство к Серверу мобильных устройств Exchange ActiveSync, пользователь с мобильного устройства подключается к своему почтовому ящику Microsoft Exchange, используя ActiveSync. При подключении пользователь в клиенте ActiveSync должен указать параметры подключения, например, адрес электронной почты, пароль электронной почты.

Мобильное устройство пользователя, подключенное к серверу Microsoft Exchange, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

После подключения мобильного устройства Exchange ActiveSync к Серверу мобильных устройств Exchange ActiveSync администратор может управлять подключенным мобильным устройством Exchange ActiveSync (см. раздел "Управление мобильными устройствами Exchange ActiveSync" на стр. 699).

Настройка веб-сервера Internet Information Services

При использовании Microsoft Exchange Server версий 2010 и 2013 в настройках веб-сервера Internet Information Services (IIS) необходимо активировать механизм аутентификации Windows для виртуальной директории Windows PowerShell™. Активация этого механизма аутентификации выполняется автоматически, если в мастере установки Сервера мобильных устройств Exchange ActiveSync установлен флажок **Настроить Microsoft Internet Information Services (IIS) автоматически** (поведение по умолчанию).

В противном случае необходимо активировать механизм аутентификации самостоятельно.

► *Чтобы активировать механизм аутентификации Windows для виртуальной директории PowerShell вручную, выполните следующие действия:*

1. В консоли Internet Information Services Manager откройте свойства виртуальной директории PowerShell.
2. Перейдите в раздел **Authentication**.
3. Выберите **Microsoft Windows Authentication** и нажмите на кнопку **Enable**.
4. Откройте дополнительные параметры **Advanced Settings**.
5. Установите флажок **Enable Kernel-mode authentication**.
6. В раскрывающемся списке **Extended Protection** выберите **Required**.

При использовании Microsoft Exchange Server версии 2007 настройка веб-сервера IIS не требуется.

Локальная установка Сервера мобильных устройств Exchange ActiveSync

Для локальной установки Сервера мобильных устройств Exchange ActiveSync администратор должен выполнить следующие действия:

1. Из дистрибутива Kaspersky Security Center скопировать содержимое папки

\Server\Packages\MDM4Exchange\ на клиентское устройство.

2. Запустите исполняемый файл setup.exe.

Локальная установка подразумевает два типа инсталляции:

- Стандартная установка – упрощенная установка, не требующая со стороны администратора настройки каких-либо параметров, рекомендуется в большинстве случаев.
- Расширенная установка – установка, требующая от администратора настройки следующих параметров:
  - путь для установки Сервера мобильных устройств Exchange ActiveSync;
  - режим работы Сервера мобильных устройств Exchange ActiveSync: обычный или в режиме кластера (см. раздел "Способы развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 98);
  - возможность указания учетной записи, под которой будет работать служба Сервера мобильных устройств Exchange ActiveSync (см. раздел "Учетная запись для работы службы Exchange ActiveSync" на стр. 99);
  - включение / выключение автоматической настройки веб-сервера IIS.

Мастер установки Сервера мобильных устройств Exchange ActiveSync следует запускать под учетной записью, обладающей необходимыми правами (см. раздел "Права для развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 99).

Удаленная установка Сервера мобильных устройств Exchange ActiveSync

► *Для настройки удаленной установки Сервера мобильных устройств Exchange ActiveSync администратор должен выполнить следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.
2. Во вложенной папке **Инсталляционные пакеты** открыть свойства пакета **Сервер мобильных устройств Exchange ActiveSync**.
3. Перейти в раздел **Параметры**.

   В разделе содержатся те же параметры, что и для локальной установки программы.

После настройки удаленной установки можно приступить к установке Сервера мобильных устройств Exchange ActiveSync.

► *Для установки Сервера мобильных устройств Exchange ActiveSync необходимо выполнить следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center выбрать папку **Удаленная установка**, в ней вложенную папку **Инсталляционные пакеты**.
2. Во вложенной папке **Инсталляционные пакеты** выбрать пакет **Сервер мобильных устройств**

Exchange ActiveSync.

3. Открыть контекстное меню пакета и выбрать пункт **Установить программу**.
4. В открывшемся мастере удаленной установки выбрать одно устройство (или несколько устройств при установке в режиме кластера).
5. В поле **Запускать инсталлятор программы под указанной учетной записью** указать учетную запись, под которой будет запущен процесс установки на удаленном устройстве.

   Учетная запись должна обладать необходимыми правами (см. раздел "Права для развертывания Сервера мобильных устройств Exchange ActiveSync" на стр. 99).

Развертывание системы управления по протоколу iOS MDM

Kaspersky Security Center позволяет управлять мобильными устройствами на платформе iOS. Мобильными устройствами iOS MDM называются мобильные устройства iOS, подключенные к Серверу iOS MDM и находящиеся под управлением Сервера администрирования.

Подключение мобильных устройств к Серверу iOS MDM выполняется в следующей последовательности:

1. Администратор устанавливает на выбранное клиентское устройство Сервер iOS MDM. Установка Сервера iOS MDM выполняется штатными средствами операционной системы.
2. Администратор получает сертификат Apple Push Notification Service (APNs-сертификат) (см. раздел "Получение APNs-сертификата" на стр. 163).

   APNs-сертификат позволяет Серверу администрирования подключаться к серверу APNs для отправки push-уведомлений на мобильные устройства iOS MDM.
3. Администратор устанавливает на Сервере iOS MDM APNs-сертификат (см. раздел "Установка сертификата APNs на Сервер iOS MDM" на стр. 166).
4. Администратор формирует iOS MDM-профиль для пользователя мобильного устройства iOS.

   iOS MDM-профиль содержит набор параметров подключения мобильных устройств iOS к Серверу администрирования.
5. Администратор выписывает пользователю общий сертификат (см. раздел "Выписка и установка общего сертификата на мобильное устройство" на стр. 168).

   Общий сертификат необходим для подтверждения того, что мобильное устройство принадлежит пользователю.
6. Пользователь переходит по ссылке, высланной администратором, и загружает установочный пакет на мобильное устройство.

   Установочный пакет содержит сертификат и iOS MDM-профиль.

   После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство iOS MDM отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.
7. Администратор добавляет конфигурационный профиль на Сервер iOS MDM и после подключения

мобильного устройства устанавливает на него конфигурационный профиль.

Конфигурационный профиль содержит набор параметров и ограничений для мобильного устройства iOS MDM, например, параметры установки приложений и использования различных функций устройства, параметры работы с электронной почтой и календарем. Конфигурационный профиль позволяет настраивать мобильные устройства iOS MDM в соответствии с политиками безопасности организации.

8. При необходимости администратор добавляет на Сервер iOS MDM provisioning-профили, а затем устанавливает provisioning-профили на мобильные устройства.

   Provisioning-профиль – это профиль, который используется для управления приложениями, распространяемыми не через App Store®. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

В этом разделе

Инсталляция Сервера iOS MDM

► *Чтобы установить Сервер iOS MDM на локальное устройство, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

   В окне с выбором программ по ссылке **Установить Сервер iOS MDM** запустите мастер установки Сервера iOS MDM.

2. Выберите папку назначения.

   Папка назначения по умолчанию <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for

iOS. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

3. В окне мастера **Параметры подключения к Серверу iOS MDM** в поле **Внешний порт подключения к службе iOS MDM** укажите внешний порт для подключения мобильных устройств к службе iOS MDM.

   Внешний порт 5223 используется мобильными устройствами для связи с APNs-сервером. Убедитесь, что в сетевом экране открыт порт 5223 для подключения к диапазону адресов 17.0.0.0/8.
   Для подключения устройства к Серверу iOS MDM по умолчанию используется порт 443. Если порт 443 уже используется другим сервисом или приложением, то его можно изменить, например, на порт 9443.
   Сервер iOS MDM использует внешний порт 2195 для отправки уведомлений на APNs-сервер. APNs-серверы работают в режиме сбалансированной нагрузки. Мобильные устройства не всегда подключаются к одним и тем же IP-адресам для получения уведомлений. Диапазон адресов 17.0.0.0/8 назначен компании Apple, поэтому рекомендуется указать весь этот диапазон как разрешенный в параметрах сетевого экрана.

4. Если вы хотите вручную настроить порты для взаимодействия между компонентами программы, установите флажок **Настроить локальные порты вручную**, а затем укажите значения следующих параметров:

   - **Порт подключения к Агенту администрирования**. Укажите в поле порт подключения службы iOS MDM к Агенту администрирования. По умолчанию установлен порт 9799.
   - **Локальный порт подключения к службе iOS MDM**. Укажите в поле локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию установлен порт 9899.

   Рекомендуется использовать значения по умолчанию.

5. В окне мастера **Внешний адрес Сервера мобильных устройств** в поле **Веб-адрес удаленного соединения с Сервером мобильных устройств** укажите адрес клиентского устройства, на котором будет установлен Сервер iOS MDM.

   Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM-устройств.

   Вы можете указать адрес клиентского устройства в одном из следующих форматов:

   - FQDN-имя устройства (например, mdm.example.com);
   - NetBIOS-имя устройства;
   - IP-адрес устройства.

> Не следует включать в строку с адресом URL-схему и номер порта: эти значения будут добавлены автоматически.

В результате работы мастера Сервер iOS MDM будет установлен на локальное устройство. Сервер iOS MDM отображается в папке **Управление мобильными устройствами** дерева консоли.

Установка Сервера iOS MDM в неинтерактивном режиме

Kaspersky Security Center позволяет устанавливать Сервер iOS MDM на локальное устройство в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Сервер iOS MDM на локальное устройство в неинтерактивном режиме,*

Выполните следующую команду:

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <setup_parameters>"
```

где `setup_parameters` – перечень параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера iOS MDM в неинтерактивном режиме, приведены в таблице ниже. Параметры можно указывать в любом порядке.

Таблица 33. Параметры установки Сервера iOS MDM в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения. Этот параметр является обязательным.	• 1 – Я принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
DONT_USE_ANSWER_FILE	Использовать xml-файл с параметрами установки Сервера iOS MDM или нет. xml-файл идет в комплекте с инсталляционным пакетом или находится на Сервере администрирования. Дополнительно путь к файлу указывать не нужно. Этот параметр является обязательным.	• 1 – не использовать XML-файл с параметрами. • Другое значение или не задано – использовать XML-файл с параметрами.

Имя параметра	Описание параметра	Возможные значения
INSTALLDIR	Папка установки Сервера iOS MDM. Этот параметр является необязательным.	Строковое значение, например, `INSTALLDIR=\"C:\install\".`
CONNECTORPORT	Локальный порт подключения службы iOS MDM к Агенту администрирования. По умолчанию установлен порт 9799. Этот параметр является необязательным.	Числовое значение.
LOCALSERVERPORT	Локальный порт подключения Агента администрирования к службе iOS MDM. По умолчанию установлен порт 9899. Этот параметр является необязательным.	Числовое значение.
EXTERNALSERVERPORT	Порт для подключения устройства к Серверу iOS MDM. По умолчанию установлен порт 443. Этот параметр является необязательным.	Числовое значение.

Имя параметра	Описание параметра	Возможные значения
EXTERNAL_SERVER_URL	Внешний адрес клиентского устройства, на котором будет установлен Сервер iOS MDM. Этот адрес будет использоваться для подключения управляемых мобильных устройств к службе iOS MDM. Клиентское устройство должно быть доступно для подключения к нему iOS MDM. Адрес не должен включать URL-схему и номер порта, так как эти значения будут добавлены автоматически. Этот параметр является необязательным.	• FQDN-имя устройства (например, mdm.example.com); • NetBIOS-имя устройства; • IP-адрес устройства.
WORKFOLDER	Рабочая папка Сервера iOS MDM. Если рабочая папка не указана, данные будут записаны в папку по умолчанию. Этот параметр является необязательным.	Строковое значение, например, `WORKFOLDER=\"C:\work\".`
MTNCY	Использование Сервера iOS MDM несколькими виртуальными Серверами. Этот параметр является необязательным.	• 1 – Сервер iOS MDM будет использоваться несколькими виртуальными Серверами администрирования. • Другое значение или не задано – Сервер iOS MDM не будет использоваться несколькими виртуальными Серверами администрирования.

Пример:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Параметры установки Сервера iOS MDM подробно описаны в разделе "Установка Сервера iOS MDM" на стр. 155.

Схемы развертывания Сервера iOS MDM

Количество установленных копий Сервера iOS MDM может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества обслуживаемых мобильных устройств.

Следует учесть, что на одну установку Kaspersky Device Management для iOS рекомендуется не более 50 000 мобильных устройств. С целью уменьшения нагрузки все множество устройств можно распределить между несколькими серверами с установленным Сервером iOS MDM.

Аутентификация iOS MDM-устройств осуществляется при помощи сертификатов пользователей (профиль, устанавливаемый на устройство, содержит сертификат того пользователя, которому оно принадлежит). Поэтому возможны две схемы развертывания Сервера iOS MDM:

- упрощенная схема;
- схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD).

Ниже рассмотрены обе схемы развертывания.

См. также:

Упрощенная схема развертывания

При развертывании Сервера iOS MDM по упрощенной схеме мобильные устройства напрямую подключаются к веб-сервису iOS MDM. При этом для аутентификации устройств могут быть использованы только пользовательские сертификаты, выпущенные Сервером администрирования. Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, PKI) для пользовательских сертификатов невозможна (см. раздел "Типовая конфигурация: Kaspersky Device Management для iOS в демилитаризованной зоне" на стр. 102).

Схема развертывания с использованием принудительного делегирования Kerberos Constrained Delegation (KCD)

Для использования схемы развертывания с принудительным делегированием Kerberos Сервер администрирования и Сервер iOS MDM должны располагаться во внутренней сети организации.

Эта схема развертывания предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (далее TMG);
- использование для аутентификации мобильных устройств принудительного делегирования Kerberos Constrained Delegation;
- интеграцию с инфраструктурой открытых ключей (PKI) для использования пользовательских сертификатов.

При использовании этой схемы развертывания следует учесть следующее:

- В Консоли администрирования в настройках веб-сервиса iOS MDM необходимо установить флажок **Обеспечить совместимость с Kerberos Constrained Delegation**.
- В качестве сертификата веб-сервиса iOS MDM следует указать особый (кастомизированный) сертификат, заданный на TMG при публикации веб-сервиса iOS MDM.
- Пользовательские сертификаты для iOS-устройств должны выписываться доменным Центром сертификации (Certification authority, далее CA). Если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны CA, указанным при публикации веб-сервиса iOS MDM на TMG.

  Обеспечить соответствие пользовательского сертификата указанному требованию возможно несколькими способами:

  - Указать пользовательский сертификат в мастере создания iOS MDM-профиля и в мастере установки сертификатов.
  - Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:

    1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
    2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
    3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
    4. В разделе **Выпуск мобильных сертификатов** укажите источник сертификатов.

См. разделы:

- Типовая конфигурация: Сервер iOS MDM в локальной сети организации (на стр. 102).
- Интеграция с инфраструктурой открытых ключей (на стр. 175).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- веб-сервис iOS MDM запущен на 443 порте;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с веб-сервисом iOS MDM – iosmdm.mydom.local;
- имя внешней публикации веб-сервиса iOS MDM – iosmdm.mydom.global.

Service Principal Name для http/iosmdm.mydom.local

В домене требуется прописать Service Principal Name (SPN) для устройства с веб-сервисом iOS MDM (iosmdm.mydom.local):

setspn -a http/iosmdm.mydom.local iosmdm

Настройка доменных свойств устройств с TMG (tmg.mydom.local)

Для делегирования трафика доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/iosmdm.mydom.local).

► *Чтобы доверить устройство с TMG службе, определенной по SPN (http/iosmdm.mydom.local), администратор должен выполнить следующие действия:*

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" необходимо выбрать устройство с установленным TMG (tmg.mydom.local).
2. В свойствах устройства на закладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.
3. В список **Services to which this account can present delegated credentials** добавить SPN http/iosmdm.mydom.local.

Особый (кастомизированный) сертификат для публикуемого веб-сервиса (iosmdm.mydom.global)

Требуется выписать особый (кастомизированный) сертификат для веб-сервиса iOS MDM на FQDN iosmdm.mydom.global и указать его взамен сертификата по умолчанию в настройках веб-сервиса iOS MDM в Консоли администрирования.

Следует учесть, что в контейнере с сертификатом (файл с расширением p12 или pfx) также должна присутствовать цепочка корневых сертификатов (публичные части).

Публикации веб-сервиса iOS MDM на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 443 порт iosmdm.mydom.global, необходимо настроить KCD на SPN http/iosmdm.mydom.local с использованием сертификата, выписанного для FQDN iosmdm.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемом веб-сервисе должен быть один и тот же серверный сертификат.

Использование Сервера iOS MDM несколькими виртуальными Серверами

► *Чтобы включить использование Сервера iOS MDM несколькими виртуальными Серверами*

администрирования, выполните следующие действия:

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
3. Для ключа ConnectorFlags (DWORD) установите значение 02102482.
4. Перейдите в раздел:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0
5. Для ключа ConnInstalled (DWORD) установите значение 00000001.
6. Перезапустите службу Сервера iOS MDM.

Задавать значения ключей необходимо в указанной последовательности.

Получение APNs-сертификата

После создания Certificate Signing Request (далее CSR-запрос) на первом шаге мастера получения APNs-сертификата приватная часть будущего сертификата (private key) сохраняется в оперативной памяти устройства. Поэтому все шаги мастера должны быть завершены в рамках одной сессии работы с программой.

► *Чтобы получить APNs-сертификат, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Запросить новый**.

   Запустится мастер получения APNs-сертификата, откроется окно **Запросить новый**.
6. Создайте Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:
   a. Нажмите на кнопку **Создать CSR**.
   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.

c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.

7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

> Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование Управления мобильными устройствами.

После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".

8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc. https://identity.apple.com/pushcert, используя произвольный Apple ID.

> Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:

a. В окне **Запрос нового APNs-сертификата** нажмите на кнопку **Завершить CSR**.

b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

Запустится экспорт сертификата.

c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **ОК**.

Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.

d. В открывшемся окне **Сохранение APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX. После этого можно установить полученный APNs-сертификат на Сервер iOS MDM (см. раздел "Установка сертификата APNs на Сервер iOS MDM" на стр. 166).

Подробнее о создании файла CSR-запроса и отправке его в Apple Inc. можно прочитать в Базе знаний на веб-сайте Службы технической поддержки "Лаборатории Касперского" http://support.kaspersky.com/14759.

См. также:

Обновление APNs-сертификата 165

Обновление APNs-сертификата

► *Чтобы обновить APNs-сертификат, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.
5. В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Обновить**.

   Запустится мастер обновления APNs-сертификата, откроется окно **Обновление APNs-сертификата**.
6. Создайте Certificate Signing Request (далее CSR-запрос). Для этого выполните следующие действия:
   a. Нажмите на кнопку **Создать CSR**.
   b. В открывшемся окне **Создание CSR** укажите название запроса, название компании и департамента, город, область и страну.
   c. Нажмите на кнопку **Сохранить** и укажите имя файла, в котором будет сохранен CSR-запрос.

   Приватная часть (private key) будущего сертификата будет сохранена в памяти устройства.
7. Отправьте созданный файл с CSR-запросом на подпись в "Лабораторию Касперского" через ваш CompanyAccount.

   > Подписание CSR-запроса доступно только после загрузки на портал CompanyAccount ключа, разрешающего использование Управления мобильными устройствами.

   После обработки вашего электронного запроса вы получите файл CSR-запроса, подписанный "Лабораторией Касперского".
8. Отправьте подписанный файл CSR-запроса на веб-сайт Apple Inc. https://identity.apple.com/pushcert, используя произвольный Apple ID.

> Не рекомендуется использовать персональный Apple ID. Создайте отдельный Apple ID, чтобы использовать его как корпоративный. Созданный Apple ID привяжите к почтовому ящику организации, а не отдельного сотрудника.

После обработки CSR-запроса в Apple Inc. вы получите публичную часть APNs-сертификата. Сохраните полученный файл на диск.

9. Запросите публичную часть сертификата. Для этого выполните следующие действия:
   a. Перейдите на портал Apple Push Certificates https://identity.apple.com/pushcert. Для авторизации на портале потребуется Apple Id, полученный при первичном запросе сертификата.
   b. В списке сертификатов выберите сертификат, APSP-имя которого (имя в формате "APSP: <номер>") совпадает с APSP-именем сертификата, используемого Сервером iOS MDM, и нажмите на кнопку **Обновить**.

      APNs-сертификат будет обновлен.
   c. Сохраните созданный порталом сертификат.
10. Экспортируйте APNs-сертификат вместе с приватным ключом, созданным при формировании CSR-запроса, в файл формата PFX. Для этого выполните следующие действия:
   a. В окне **Обновление APNs-сертификата** нажмите на кнопку **Завершить CSR**.
   b. В открывшемся окне **Открыть** выберите файл с публичной частью сертификата, полученный после обработки CSR-запроса в Apple Inc., и нажмите на кнопку **Открыть**.

      Запустится экспорт сертификата.
   c. В открывшемся окне введите пароль для приватного ключа, нажмите на кнопку **ОК**.

      Заданный пароль будет использоваться для установки APNs-сертификата на Сервер iOS MDM.
   d. В открывшемся окне **Обновление APNs-сертификата** укажите имя файла для сохранения APNs-сертификата, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Приватная и публичная части сертификата будут объединены, APNs-сертификат будет сохранен в файл формата PFX.

См. также:

Получение APNs-сертификата.....163

Установка сертификата APNs на Сервер iOS MDM

После получения APNs-сертификата необходимо установить APNs-сертификат на Сервер iOS MDM.

► *Чтобы установить APNs-сертификат на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
2. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
3. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
4. В окне свойств Сервера iOS MDM выберите раздел **Сертификаты**.

В разделе **Сертификаты** в блоке параметров **Сертификат Apple Push Notification** нажмите на кнопку **Установить**.

1. Выберите файл формата PFX, содержащий APNs-сертификат.
2. Введите пароль приватного ключа, указанный при экспорте APNs-сертификата (см. раздел "Получение APNs-сертификата" на стр. 163).

В результате APNs-сертификат будет установлен на Сервер iOS MDM. Информация о сертификате будет отображаться в окне свойств Сервера iOS MDM в разделе **Сертификаты**.

Настройка доступа к сервису Apple Push Notification

Для корректной работы веб-сервиса iOS MDM, а также для обеспечения своевременного реагирования мобильных устройств на команды администратора, в параметрах Сервера iOS MDM следует указать сертификат Apple Push Notification Service (далее APNs-сертификат).

О том, как получить APNs-сертификат см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/14759.

Взаимодействуя с сервисом Apple Push Notification (далее APNs), веб-сервис iOS MDM подключается к внешнему адресу gateway.push.apple.com по порту 2195 (исходящий). Поэтому веб-сервису iOS MDM необходимо предоставить доступ к порту TCP 2195 для диапазона адресов 17.0.0.0/8. Со стороны iOS устройства – доступ к порту TCP 5223 для диапазона адресов 17.0.0.0/8.

Если доступ к APNs со стороны веб-сервиса iOS MDM предполагается осуществлять через прокси-сервер, то на устройстве с установленным веб-сервисом iOS MDM необходимо выполнить следующие действия:

1. Прописать в Реестр следующие строки:
   - Для 32-разрядной операционной системы:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

- Для 64-разрядной операционной системы:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

2. Перезапустить службу веб-сервиса iOS MDM.

Выписка и установка общего сертификата на мобильное устройство

► *Чтобы выписать общий сертификат пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите учетную запись пользователя.
2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера сертификат будет создан и добавлен в список сертификатов пользователя (см. раздел "Работа с сертификатами" на стр. 684).

Выписанный сертификат пользователь загружает вместе с установочным пакетом, в котором содержится iOS MDM-профиль.

После подключения мобильного устройства к Серверу iOS MDM на устройстве пользователя будут применены параметры iOS MDM-профиля. Администратор сможет управлять подключенным устройством.

Мобильное устройство пользователя, подключенное к Серверу iOS MDM, отображается в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление KES-устройства в список управляемых устройств

► *Чтобы добавить KES-устройство пользователя в список управляемых устройств с помощью ссылки на Google Play™, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

   Запустится мастер добавления мобильных устройств. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на устройство;
   - указать файл общего сертификата.

4. В окне мастера **Тип устройства** выберите вариант **Ссылка на Google Play**.

5. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата (с помощью SMS-сообщения, по электронной почте или информация будет отображена после окончания работы мастера).

6. В окне мастера Информация о сертификате нажмите на кнопку **Готово** для завершения работы мастера.

В результате работы мастера на устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android с Google Play. Пользователь переходит в магазин приложений Google Play по ссылке или отсканировав QR-код. После этого операционная система устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если приложение Kaspersky Endpoint Security для Android уже установлено на устройство, пользователю нужно самостоятельно ввести параметры подключения к Серверу администрирования, получив их у администратора. После настройки параметров подключения мобильное устройство подключается к Серверу администрирования. Администратор выписывает общий сертификат для устройства и отправляет пользователю сообщение электронной почты или SMS с именем пользователя и паролем для загрузки сертификата. Пользователь загружает и устанавливает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Повторная загрузка и установка Kaspersky Endpoint Security для Android в этом случае не выполняются.

Подключение KES-устройств к Серверу администрирования

В зависимости от способа подключения устройств к Серверу администрирования существует две схемы развертывания Kaspersky Device Management для iOS для KES-устройств:

- схема развертывания с использованием прямого подключения устройств к Серверу администрирования;
- схема развертывания с использованием Forefront® Threat Management Gateway (TMG).

В этом разделе

Прямое подключение устройств к Серверу администрирования

KES-устройства могут напрямую подключаться к порту 13292 Сервера администрирования.

В зависимости от способа аутентификации существуют два варианта подключения KES-устройств к Серверу администрирования:

- подключение устройств с использованием пользовательского сертификата;
- подключение устройств без пользовательского сертификата.

Подключение устройства с использованием пользовательского сертификата

При подключении устройства с использованием пользовательского сертификата происходит привязка этого устройства к учетной записи пользователя, для которой средствами Сервера администрирования назначен соответствующий сертификат.

В этом случае будет использована двусторонняя аутентификация SSL (2-way SSL authentication, mutual authentication). Как Сервер администрирования, так и устройство будут аутентифицированы с помощью сертификатов.

Подключение устройства без пользовательского сертификата

При подключении устройства без пользовательского сертификата оно не будет привязано ни к одной учетной записи пользователя на Сервере администрирования. Но при получении устройством любого сертификата будет произведена привязка этого устройства к пользователю, которому средствами Сервера администрирования назначен соответствующий сертификат.

При подключении устройства к Серверу администрирования будет использована односторонняя SSL-аутентификация (1-way SSL authentication), при которой только Сервер администрирования аутентифицируется с помощью сертификата. После получения устройством пользовательского сертификата тип аутентификации будет изменен на двустороннюю аутентификацию SSL (2-way SSL authentication, mutual authentication (см. раздел "Предоставление доступа к Серверу администрирования из интернета" на стр. 84)).

Схема подключения KES-устройств к Серверу с использованием принудительного делегирования Kerberos (KCD)

Схема подключения KES-устройств к Серверу администрирования с использованием Kerberos Constrained Delegation (KCD) предполагает:

- интеграцию с Microsoft Forefront Threat Management Gateway (далее TMG);
- использование принудительного делегирования Kerberos Constrained Delegation (далее KCD) для аутентификации мобильных устройств;
- интеграцию с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) для использования пользовательских сертификатов.

При использовании этой схемы подключения следует учесть следующее:

- Тип подключения KES-устройств к TMG должен быть "2-way SSL authentication", то есть устройство должно подключаться к TMG по своему пользовательскому сертификату. Для этого в инсталляционный пакет Kaspersky Endpoint Security для Android, который установлен на устройстве, необходимо интегрировать пользовательский сертификат. Этот KES-пакет должен быть создан Сервером администрирования специально для данного устройства (пользователя).
- Вместо серверного сертификата по умолчанию для мобильного протокола следует указать особый (кастомизированный) сертификат:
  1. В окне свойств Сервера администрирования в разделе **Параметры** установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.
  2. В открывшемся окне указать тот же сертификат, что задан на TMG при публикации точки доступа к мобильному протоколу на Сервере администрирования.
- Пользовательские сертификаты для KES-устройств должны выписываться доменным Certificate Authority (CA). Причем следует учесть, что если в домене несколько корневых CA, то пользовательские сертификаты должны быть выписаны тем CA, который прописан в публикации на

TMG.

Обеспечить соответствие пользовательского сертификата заявленному выше требованию возможно несколькими способами:

- Указать особый пользовательский сертификат в мастере создания инсталляционных пакетов и в мастере установки сертификатов.
- Интегрировать Сервер администрирования с доменным PKI и настроить соответствующий параметр в правилах выписки сертификатов:
  1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
  2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
  3. В разделе **Интеграция с PKI** настройте интеграцию с инфраструктурой открытых ключей.
  4. В разделе **Выпуск мобильных сертификатов** укажите источник сертификатов.

См. разделы:

- Интеграция с инфраструктурой открытых ключей (на стр. 175).
- Предоставление доступа к Серверу администрирования из интернета (на стр. 84).

Рассмотрим пример настройки ограниченного делегирования KCD со следующими допущениями:

- точка доступа к мобильному протоколу на Сервере администрирования поднята на 13292 порте;
- имя устройства с TMG – tmg.mydom.local;
- имя устройства с Сервером администрирования – ksc.mydom.local;
- имя внешней публикации точки доступа к мобильному протоколу – kes4mob.mydom.global.

Доменная учетная запись для Сервера администрирования

Необходимо создать доменную учетную запись (например, KSCMobileSrvcUsr), под которой будет работать служба Сервера администрирования. Указать учетную запись для службы Сервера администрирования можно при установке Сервера администрирования или с помощью утилиты klsrvswch. Утилита klsrvswch расположена в папке установки Сервера администрирования.

Указать доменную учетную запись необходимо по следующим причинам:

- Функциональность по управлению KES-устройствами является неотъемлемой частью Сервера администрирования.
- Для правильной работы принудительного делегирования (KCD) принимающая сторона, которой является Сервер администрирования, должна работать под доменной учетной записью.

Service Principal Name для http/kes4mob.mydom.local

В домене под учетной записью KSCMobileSrvcUsr требуется прописать Service Principal Name (SPN) для публикации сервиса мобильного протокола на 13292 порту устройства с Сервером администрирования. Для устройства kes4mob.mydom.local с Сервером администрирования это будет выглядеть следующим

образом:

setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr

Настройка доменных свойств устройств с TMG (tmg.mydom.local)

Для делегирования трафика нужно доверить устройство с TMG (tmg.mydom.local) службе, определенной по SPN (http/kes4mob.mydom.local:13292).

Чтобы доверить устройство с TMG службе, определенной по SPN (http/kes4mob.mydom.local:13292), администратор должен выполнить следующие действия:

1. В оснастке Microsoft Management Console "Active Directory Users and Computers" необходимо выбрать устройство с установленным TMG (tmg.mydom.local).
2. В свойствах устройства на закладке **Delegation** для переключателя **Trust this computer for delegation to specified service only** выбрать вариант **Use any authentication protocol**.
3. В список **Services to which this account can present delegated credentials** добавить SPN http/kes4mob.mydom.local:13292.

Особый (кастомизированный) сертификат для публикации (kes4mob.mydom.global)

Для публикации мобильного протокола Сервера администрирования требуется выписать особый (кастомизированный) сертификат на FQDN kes4mob.mydom.global и указать его взамен серверного сертификата по умолчанию в параметрах мобильного протокола Сервера администрирования в Консоли администрирования. Для этого в окне свойств Сервера администрирования в разделе **Параметры** необходимо установить флажок **Открыть порт для мобильных устройств** и в раскрывающемся списке выбрать **Добавить сертификат**.

Следует учесть, что в контейнере с серверным сертификатом (файл с расширением p12 или pfx) должна также присутствовать цепочка корневых сертификатов (публичные части).

Настройка публикации на TMG

На TMG для трафика, идущего со стороны мобильного устройства на 13292 порт kes4mob.mydom.global, необходимо настроить KCD на SPN http/kes4mob.mydom.local:13292 с использованием серверного сертификата, выписанного для FQND kes4mob.mydom.global. При этом следует учесть, что как на публикации, так и на публикуемой точке доступа (13292 порт Сервера администрирования) должен быть один и тот же серверный сертификат.

Использование Google Firebase Cloud Messaging

Для обеспечения своевременного реагирования KES-устройств под управлением Android на команды администратора в свойствах Сервера администрирования следует включить использование сервиса Google™ Firebase Cloud Messaging (далее FCM).

► *Чтобы включить использование FCM, выполните следующие действия:*

1. В Консоли администрирования выберите узел **Управление мобильными устройствами**, папку **Мобильные устройства**.

2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В свойствах папки выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. В полях **Идентификатор отправителя** и **Ключ сервера** укажите параметры FCM: SENDER_ID и API Key.

Сервис FCM работает на следующих диапазонах адресов:

- Со стороны KES-устройства необходим доступ на порты 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) следующих адресов:
  - google.com;
  - android.googleapis.com;
  - android.apis.google.com;
  - либо на все IP из списка "Google ASN 15169".
- Со стороны Сервера администрирования необходим доступ на порт 443 (HTTPS) следующих адресов:
  - android.googleapis.com;
  - либо на все IP из списка "Google ASN 15169".

В случае если в Консоли администрирования в свойствах Сервера администрирования заданы параметры прокси-сервера (**Дополнительно** / **Параметры доступа к сети Интернет**), то они будут использованы для взаимодействия с FCM.

Настройка FCM: получение SENDER_ID, API Key

Для настройки работы с FCM администратор должен выполнить следующие действия:

1. Зарегистрироваться на портале google https://accounts.google.com.
2. Перейти на портал для разработчиков https://console.developers.google.com/project.
3. Создать новый проект по кнопке **Create Project**, указать имя проекта и ID проекта.
4. Дождаться создания проекта.

   На первой странице проекта, в верхней части страницы, в поле **Project Number** указан искомый SENDER_ID.
5. Перейти в раздел **APIs & auth / APIs**, включить **Google Firebase Cloud Messaging for Android**.
6. Перейти в раздел **APIs & auth / Credentials** и нажать на кнопку **Create New Key**.
7. Нажать на кнопку **Server key**.
8. Если есть, задать ограничения, нажать на кнопку **Create**.
9. Получить API Key из свойств только что созданного ключа (поле **Ключ сервера**).

Интеграция с инфраструктурой открытых ключей

Интеграция с инфраструктурой открытых ключей (Public Key Infrastructure, далее PKI) в первую очередь предназначена для упрощения выпуска доменных пользовательских сертификатов Сервером администрирования.

Администратор может назначить для пользователя доменный сертификат в Консоли администрирования. Это можно сделать одним из следующих способов:

- назначить пользователю особый (кастомизированный) сертификат из файла в мастере подключения нового устройства либо в мастере установки сертификатов;
- выполнить интеграцию с PKI и назначить PKI источником сертификатов для конкретного типа сертификатов либо для всех типов сертификатов.

Параметры интеграции с PKI доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** по ссылке **Интегрировать с инфраструктурой открытых ключей**.

Общий принцип интеграции с PKI для выпуска доменных сертификатов пользователей

В Консоли администрирования по ссылке **Интегрировать с инфраструктурой открытых ключей** в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** следует задать доменную учетную запись, которая будет использована Сервером администрирования для выписки доменных пользовательских сертификатов посредством доменного CA (далее – учетная запись, под которой производится интеграция с PKI).

Обратите внимание:

- В параметрах интеграции с PKI существует возможность указать шаблон по умолчанию для всех типов сертификатов. Тогда как в правилах выпуска сертификатов (правила доступны в рабочей области папки **Управление мобильными устройствами** / **Сертификаты** по кнопке **Настроить правила выпуска сертификатов**) присутствует возможность задать шаблон для каждого типа сертификата отдельно.
- На устройстве с установленным Сервером администрирования в хранилище сертификатов учетной записи, под которой производится интеграция с PKI, должен быть установлен специализированный сертификат Enrollment Agent (EA). Сертификат Enrollment Agent (EA) выписывает администратор доменного CA (Certificate Authority).

Учетная запись, под которой производится интеграция с PKI, должна соответствовать следующим критериям:

- Является доменным пользователем.
- Является локальным администратором устройства с установленным Сервером администрирования, с которого производится интеграция с PKI.
- Обладает правом *Вход в качестве службы*.
- Под этой учетной записью необходимо хотя бы один раз запустить устройство с установленным Сервером администрирования, чтобы создать постоянный профиль пользователя.

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее Веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер предназначен для публикации автономных пакетов установки, автономных инсталляционных пакетов для мобильных устройств, iOS MDM-профилей, а также файлов из папки общего доступа.

Созданные iOS MDM-профили и инсталляционные пакеты публикуются на Веб-сервере автоматически и удаляются после первой загрузки. Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на мобильное устройство предназначенную для него информацию.

Настройка Веб-сервера

Для тонкой настройки Веб-сервера в свойствах Веб-сервера Консоли администрирования предусмотрена возможность смены портов для протоколов HTTP (8060) и HTTPS (8061). Также, помимо смены портов, возможна смена серверного сертификата для HTTPS-протокола и смена FQDN-имени веб-сервера для HTTP-протокола.

Установка Kaspersky Security Center

В этом разделе описывается локальная установка компонентов Kaspersky Security Center. Доступны два типа установки:

- **Обычный**. Этот вариант рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор модулей управления, заданный по умолчанию, для программ "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.
- **Пользовательская**. Этот вариант рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в неинтерактивном режиме (см. раздел "Установка в неинтерактивном режиме" на стр. 200).

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом форсированной установки (см. раздел "Установка программ с помощью задачи удаленной установки" на стр. 272). При формировании задачи удаленной установки следует использовать инсталляционный пакет Сервера администрирования.

Вы можете использовать один из двух типов установочных пакетов:

- ksc_11.<номер сборки>_full_<язык локализации>.exe. Содержит полный набор компонентов для установки. Используйте этот пакет, если вы хотите установить все компоненты, необходимые для работы всех функций Kaspersky Security Center, или обновить существующие версии этих компонентов.
- ksc_11.<номер сборки>_lite_<язык локализации>.exe. Содержит минимальный набор компонентов, необходимый для работы Kaspersky Security Center. Например, этот пакет не содержит плагинов управления программой Kaspersky Endpoint Security 10 для Windows.

  Используйте этот пакет установки, если:

  - вы хотите обновить Сервер администрирования с предыдущей версии;
  - у вас уже установлены компоненты, необходимые для полной функциональности Kaspersky Security Center, и вы хотите продолжить пользоваться существующими версиями этих компонентов;
  - вы хотите использовать Kaspersky Security Center с ограниченной функциональностью;
  - вы собираетесь использовать Kaspersky Security Center в организациях, где ограничен интернет-трафик и дистрибутивы загружаются отдельно.

В этом разделе

Подготовка к установке

Перед началом установки нужно убедиться, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования.

Kaspersky Security Center хранит информацию в базе данных SQL-сервера. Для этого необходимо самостоятельно установить базу данных SQL-сервера (подробнее о выборе СУБД (см. раздел "О выборе СУБД для Сервера администрирования" на стр. 82)). Для хранения информации можно использовать и другие SQL-серверы. Они должны быть установлены в сети до начала установки Kaspersky Security Center. Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

Если используется чувствительность к регистру, Kaspersky Security Center может не обнаружить некоторые уязвимости. Не устанавливайте Сервер администрирования и Агент администрирования в папки с включенной чувствительностью к регистру.

Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно.

Учетные записи для работы с СУБД

В таблицах ниже приведена информация о том, как влияет выбор системы управления базами данных (СУБД) на свойства учетных записей для работы с СУБД.

Локальной СУБД называется СУБД, установленная на том же устройстве, что и Сервер администрирования. Удаленной СУБД называется СУБД, установленная на другом устройстве.

Задавайте все права, необходимые для учетной записи Сервера администрирования, до запуска службы Сервера администрирования.

SQL Server с аутентификацией Windows и с аутентификацией SQL Server

Таблица 34. SQL Server (в том числе и Express Edition) с аутентификацией Windows

Расположение СУБД	Локальная	Локальная	Удаленная	Удаленная
Кто создает базу данных KAV	Инсталлятор (автоматически)	Администратор вручную	Инсталлятор (автоматически)	Администратор вручную
Учетная запись, от имени которой работает инсталлятор	Локальная или доменная	Локальная или доменная	Доменная	Доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • SQL Server: роль sysadmin.	• Системные: права локального администратора. • SQL-сервер: схема dbo для базы данных KAV; роли db_datareader и db_datawriter для каждой из баз данных KAV, master и tempdb.	• Системные: права локального администратора. • SQL Server: роль sysadmin.	• Системные: права локального администратора. • SQL-сервер: схема dbo для базы данных KAV; роли db_datareader и db_datawriter для каждой из баз данных KAV, master и tempdb.

Учетная запись Сервера администрирования	• Автоматически созданная вида KL-AK-*. • Выбранная администратором локальная. • Выбранная администратором доменная.	• Автоматически созданная вида KL-AK-*. • Выбранная администратором локальная. • Выбранная администратором доменная.	Доменная	Доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: необходимые права, присвоенные инсталлятором.	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: администратор должен присвоить учетной записи роль db_owner для базы данных KAV и роли db_datareader и db_datawriter для каждой из баз данных master и tempdb. Если используется AlwaysOn, на SQL-сервере необходимо предоставить разрешение VIEW SERVER STATE.	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: необходимые права, присвоенные инсталлятором.	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: администратор должен присвоить учетной записи роль db_owner для базы данных KAV, роли db_datareader и db_datawriter для каждой из баз данных master и tempdb. Если используется AlwaysOn, на SQL-сервере необходимо предоставить разрешение VIEW SERVER STATE.

Таблица 35. SQL Server (в том числе и Express Edition) с аутентификацией SQL Server

Расположение СУБД	Локальная	Удаленная

Кто создает базу данных KAV	Администратор (вручную) или инсталлятор (автоматически)	Администратор (вручную) или инсталлятор (автоматически)
Учетная запись, от имени которой работает инсталлятор	Локальная	Доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • SQL-сервер: учетной записи инсталлятора не требуется доступ к SQL Server.	• Системные: права локального администратора. • SQL-сервер: учетной записи инсталлятора не требуется доступ к SQL Server.
Учетная запись службы Сервера администрирования	Локальная или доменная	Доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: учетной записи службы Сервера администрирования не требуется доступ к SQL Server.	• Системные: необходимые права, присвоенные инсталлятором. • SQL Server: учетной записи службы Сервера администрирования не требуется доступ к SQL Server.
Дополнительная информация	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, для которой необходима роль sysadmin.	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, для которой необходима роль sysadmin.

MySQL

Таблица 36. СУБД: MySQL

Расположение СУБД	Локальная или удаленная	Локальная или удаленная
Кто создает базу данных KAV	Инсталлятор (автоматически)	Администратор вручную
Учетная запись, от имени которой работает инсталлятор	Локальная или доменная	Локальная или доменная
Права учетной записи, от имени которой работает инсталлятор	• Системные: права локального администратора. • MySQL Server: учетной записи инсталлятора не требуется доступ к MySQL.	• Системные: права локального администратора. • MySQL Server: учетной записи инсталлятора не требуется доступ к MySQL.

Учетная запись службы Сервера администрирования	Локальная или доменная	Локальная или доменная
Права учетной записи службы Сервера администрирования	• Системные: необходимые права, присвоенные инсталлятором. • MySQL Server: учетной записи службы Сервера администрирования не требуется доступ к MySQL.	• Системные: необходимые права, присвоенные инсталлятором. • MySQL Server: учетной записи службы Сервера администрирования не требуется доступ к MySQL.
Дополнительная информация	Администратор явным образом задает в инсталляторе внутреннюю учетную запись SQL Server, для которой необходим доступ root.	Администратор явным образом задает в инсталляторе внутреннюю учетную запись MySQL, для которой необходим доступ GRANT ALL для базы данных KAV, а также права SELECT, SHOW VIEW, PROCESS на системные таблицы.

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

В этом разделе

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins.
2. Задать в инсталляторе Сервера администрирования доменные учетные записи, созданные для служб (см. раздел "Шаг 7. Выбор учетной записи для запуска служб Kaspersky Security Center"" на стр. 195).

Задание папки общего доступа

Во время установки Сервера администрирования можно задать месторасположение папки общего доступа. Также месторасположение папки общего доступа можно задать после установки, в свойствах Сервера администрирования. По умолчанию папка общего доступа создается на устройстве с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (высокая нагрузка, необходимость доступа из изолированной сети и прочее) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

См. также:

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory 183

Удаленная инсталляция рассылкой UNC-пути на автономный пакет 184

Обновление из папки общего доступа Сервера администрирования 184

Установка образов операционных систем 90

Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если устройства находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и программы безопасности на пока еще не управляемые устройства) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему устройства с Сервером администрирования

целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Удаленная инсталляция рассылкой UNC-пути на автономный пакет

В случае если пользователи устройств сети организации имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже "спаренного" пакета Агента администрирования совместно с программой безопасности). После создания автономного пакета нужно отправить пользователям устройств сети ссылку на пакет, находящийся в папке общего доступа. Инсталляция запускается по ссылке.

Обновление из папки

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества устройств, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: устройства читают из папки образы операционных систем. Если планируется развертывание образов на большом количестве устройств организации, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

См. также:

Развертывание Агента администрирования и программы безопасности 108

Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. По умолчанию используется NetBIOS-имя устройства с Сервером администрирования. Если в сети организации настроена и правильно работает DNS, то следует здесь задать FQDN-имя устройства с Сервером администрирования. Если Сервер администрирования установлен в демилитаризованной зоне, то может быть целесообразным указать внешний адрес Сервера администрирования. В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

См. также:

Стандартная установка

Стандартная установка – это установка Сервера администрирования, при которой используются заданные по умолчанию пути для файлов программы, устанавливается набор плагинов по умолчанию и не включается Управление мобильными устройствами.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_11.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 11** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

Далее описаны шаги мастера установки программы, а также действия, которые вы можете выполнить на каждом из этих шагов.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками

конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения;**
- **Политику конфиденциальности, которая описывает обработку данных.**

Установка программы будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 2. Selecting an installation method

В окне выбора типа установки укажите тип **Стандартная**.

Стандартная установка рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Параметры Сервера администрирования не настраиваются, для них используются заданные по умолчанию значения. Стандартная установка не позволяет выбрать устанавливаемые плагины управления, устанавливается заданный по умолчанию набор плагинов. Во время стандартной установки инсталляционные пакеты для мобильных устройств не создаются. Вы можете создать их позже в Консоли администрирования.

Шаг 3. Установка Kaspersky Security Center 11 Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center 11 Web Console не работает с 32-разрядными операционными системами.

Если требуется установить Kaspersky Security Center 11 Web Console на то же устройство, что и Kaspersky Security Center, установите флажок **Установить Kaspersky Security Center 11 Web Console**. Если этот флажок не установлен, Kaspersky Security Center 11 Web Console не будет установлена. Будет установлена только Консоль администрирования на основе Microsoft Management Console (MMC). Однако если вы используете 64-разрядную операционную систему, можно установить Kaspersky Security Center 11 Web Console позже, после начала работы с Kaspersky Security Center.

Для сертифицированного состояния программы программу Kaspersky Security Center 11 Web Console устанавливать нельзя. Для этого флажок **Установить Kaspersky Security Center 11 Web Console** должен быть снят.

Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

Таблица 37. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	отсутствует	отсутствует	присутствует	присутствует
Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования	отсутствует	отсутствует	присутствует	присутствует
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Шаг 5. Выбор базы данных

На этом шаге мастера установки требуется выбрать ресурс Microsoft SQL Server (SQL Express) или MySQL, который будет использоваться для размещения информационной базы данных Сервера администрирования.

Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), для него не предусмотрена возможность установки Microsoft SQL Server (SQL Express). В этом случае для правильной установки Kaspersky Security Center рекомендуется использовать ресурс MySQL.

Структура базы данных Сервера администрирования описана в файле klakdb.chm, который расположен в папке установки программы Kaspersky Security Center (этот файл в виде архива доступен на портале "Лаборатории Касперского": klakdb.zip (http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip)).

См. также:

Выбор СУБД 82

Шаг 6. Настройка параметров SQL-сервера

На этом шаге мастера установки выполняется настройка параметров SQL-сервера.

В зависимости от выбранной базы данных возможны следующие варианты настройки параметров SQL-сервера:

- Если на предыдущем этапе вы выбрали вариант **Microsoft SQL Server (SQL Server Express)**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если Сервер администрирования запускается под учетной записью локального администратора или под учетной записью LocalSystem, кнопка **Обзор** недоступна.

    Если в сети организации установлен SQL-сервер с настроенной поддержкой AlwaysON, в поле **Имя SQL-сервера** укажите имя прослушивателя группы доступности.

  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если на предыдущем этапе был выбран вариант **MySQL**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя установленного экземпляра SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных

SQL-сервера. По умолчанию установлен порт 3306.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Security Center.

Шаг 7. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

В зависимости от выбранной базы данных вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Программа проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вы должны указать правильные учетные данные.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для сервера MySQL укажите учетную запись и пароль.

Шаг 8. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить

установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую Консоль администрирования требуется запустить для работы с Kaspersky Security Center:

- **Запустить как Консоль администрирования на основе MMC.**
- **Запустить как Kaspersky Security Center 11 Web Console.**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center 11 Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Готово**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования вы можете выполнить первоначальную настройку программы (на стр. 213).

По окончании работы мастера установки следующие компоненты программы будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования на основе консоли управления Microsoft Management Console (MMC);
- доступные в дистрибутиве плагины управления программами.

Кроме того, будет установлена программа Microsoft Windows Installer версии 4.5, если эта программа не была установлена ранее.

Выборочная установка

Выборочная установка – это установка Сервера администрирования, при которой вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлена программа.

С помощью этого типа установки вы можете настроить параметры базы данных, параметры Сервера администрирования, установить компоненты, которые не включены в стандартную установку и плагины управления защитными программами "Лаборатории Касперского". Вы можете также включить Управление мобильными устройствами.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_11.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 11** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

Далее описаны шаги мастера установки программы, а также действия, которые вы можете выполнить на каждом из этих шагов.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения;**

- **Политику конфиденциальности, которая описывает обработку данных.**

Установка программы будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 2. Selecting an installation method

В окне выбора типа установки укажите тип **Выборочная**.

Выборочная установка позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При выборочной установке вы можете создать инсталляционные пакеты для мобильных устройств, указав соответствующий параметр.

Шаг 3. Установка Kaspersky Security Center 11 Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center 11 Web Console не работает с 32-разрядными операционными системами.

Если требуется установить Kaspersky Security Center 11 Web Console на то же устройство, что и Kaspersky Security Center, установите флажок **Установить Kaspersky Security Center 11 Web Console**. Если этот флажок не установлен, Kaspersky Security Center 11 Web Console не будет установлена. Будет установлена только Консоль администрирования на основе Microsoft Management Console (MMC). Однако если вы используете 64-разрядную операционную систему, можно установить Kaspersky Security Center 11 Web Console позже, после начала работы с Kaspersky Security Center.

Для сертифицированного состояния программы программу Kaspersky Security Center 11 Web Console устанавливать нельзя. Для этого флажок **Установить Kaspersky Security Center 11 Web Console** должен быть снят.

Шаг 4. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования

(см. раздел "Создание инсталляционных пакетов программ" на стр. 670).

- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке программы на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки программы во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить нельзя.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

Шаг 5. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

Таблица 38. Зависимость параметров установки от выбора размеров сети

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами	отсутствует	отсутствует	присутствует	присутствует
Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования	отсутствует	отсутствует	присутствует	присутствует

Параметры	1–100 устройств	100–1000 устройств	1000–5000 устройств	Более 5000 устройств
Распределение времени запуска задачи обновления на клиентских устройствах случайным образом	отсутствует	в интервале 5 минут	в интервале 10 минут	в интервале 10 минут

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 5000 устройств.

Шаг 6. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Программа создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. раздел "Шаг 11.Выбор папки общего доступа" на стр. 198) и СУБД на том же устройстве, что и Сервер администрирования (см. раздел "Шаг 8. Выбор базы данных" на стр. 196).

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. раздел "Шаг 8. Выбор базы данных" на стр. 196), расположенный на другом устройстве, и / или если вы планируете разместить папку общего доступа на другом устройстве (см. раздел "Шаг 11. Выбор папки общего доступа" на стр.198).

  Kaspersky Security Center начиная с версии 10 Service Pack 3 поддерживает управляемые учетные записи службы и групповые управляемые учетные записи службы. Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования:

  1. Нажмите на кнопку **Обзор**.
  2. В появившемся окне нажмите на кнопку **Object type**.
  3. Выберите тип **Account for services** и нажмите на кнопку **OK**.
  4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. раздел "Учетные записи для работы с СУБД" на стр. 179).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch) (см. раздел "Смена учетной записи службы Сервера администрированияУтилита klsrvswch" на стр. 553).

См. также:

Учетные записи для работы с СУБД 179

Изменения в системе после установки Сервера администрирования на устройство 208

Шаг 7. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. раздел "Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере" на стр. 183).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

См. также:

Изменения в системе после установки Сервера администрирования на устройство 208

Шаг 8. Выбор базы данных

На этом шаге мастера установки требуется выбрать ресурс Microsoft SQL Server (SQL Express) или MySQL, который будет использоваться для размещения информационной базы данных Сервера администрирования.

Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), для него не предусмотрена возможность установки Microsoft SQL Server (SQL Express). В этом случае для правильной установки Kaspersky Security Center рекомендуется использовать ресурс MySQL.

Структура базы данных Сервера администрирования описана в файле klakdb.chm, который расположен в папке установки программы Kaspersky Security Center (этот файл в виде архива доступен на портале "Лаборатории Касперского": klakdb.zip (http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip)).

Шаг 9. Настройка параметров SQL-сервера

На этом шаге мастера установки выполняется настройка параметров SQL-сервера.

В зависимости от выбранной базы данных возможны следующие варианты настройки параметров SQL-сервера:

- Если на предыдущем этапе вы выбрали вариант **Microsoft SQL Server (SQL Server Express)**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если Сервер администрирования запускается под учетной записью локального администратора или под учетной записью LocalSystem, кнопка **Обзор** недоступна.

    Если в сети организации установлен SQL-сервер с настроенной поддержкой AlwaysON, в поле **Имя SQL-сервера** укажите имя прослушивателя группы доступности.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения

информации Сервера администрирования. По умолчанию указано значение *KAV*.

- Если на предыдущем этапе был выбран вариант **MySQL**, укажите следующие параметры:
  - В поле **Имя SQL-сервера** укажите имя установленного экземпляра SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных SQL-сервера. По умолчанию установлен порт 3306.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Security Center.

Шаг 10. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

В зависимости от выбранной базы данных вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Программа проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вы должны указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для сервера MySQL укажите учетную запись и пароль.

Шаг 11. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки программ (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки программных компонентов Kaspersky Security Center.

Шаг 12. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Номер порта**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- **Номер SSL-порта**

Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

По умолчанию установлен порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию выбран вариант **2048 бит (большая безопасность)**.

Если Сервер администрирования работает под управлением Microsoft Windows XP с Service Pack 2, то встроенный сетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на устройстве, на котором установлен Сервер администрирования, эти порты нужно открыть вручную.

См. также:

Порты, используемые Kaspersky Security Center 56

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Шаг 13. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена**. Этот вариант используется в том случае, когда в сети присутствует DNS-сервер, и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя**. Этот вариант используется, если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- **IP-адрес**. Этот вариант используется, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Шаг 14. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

Укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети.

Шаг 15. Выбор плагинов управления программами

Выберите плагины управления программами "Лаборатории Касперского", которые требуется установить совместно с Kaspersky Security Center.

Для удобства поиска плагины разделены на группы в зависимости от типа защищаемых объектов.

Шаг 16. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую Консоль администрирования требуется запустить для работы с Kaspersky Security Center:

- **Запустить как Консоль администрирования на основе MMC.**
- **Запустить как Kaspersky Security Center 11 Web Console.**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center 11 Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Готово**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования вы можете выполнить первоначальную настройку программы (на стр. 213).

Установка в неинтерактивном режиме

Сервер администрирования может быть установлен в неинтерактивном режиме, то есть без

интерактивного ввода параметров установки.

► *Чтобы установить Сервер администрирования на локальном устройстве в неинтерактивном режиме,*

выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1
<setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PRO1=PROP1VAL PROP2=PROP2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в неинтерактивном режиме, приведены в таблице ниже.

Таблица 39. Параметры установки Сервера администрирования в неинтерактивном режиме

Имя параметра	Описание параметра	Возможные значения
EULA	Согласие с условиями Лицензионного соглашения	• 1 – Я принимаю условия Лицензионного соглашения. • Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется).
PRIVACYPOLICY	Согласие с условиями Политики конфиденциальности	• 1 – Я принимаю условия Политики конфиденциальности. • Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется).
INSTALLATIONMODETYPE	Тип установки Сервера администрирования.	• Standard – стандартная установка. • Custom – выборочная установка.
INSTALLDIR	Путь к папке установки Сервера администрирования	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
ADDLOCAL	Список компонентов (через запятую) Сервера администрирования для установки	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 Минимальный достаточный для корректной установки Сервера администрирования список компонентов: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Размер сети (количество устройств в сети)	• NRT_1_100 – от 100 до 100 устройств. • NRT_100_1000 – от 101 до 1 000 устройств. • NRT_GREATER_1000 – более 1000 устройств.
SRV_ACCOUNT_TYPE	Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба	• SrvAccountDefault – учетная запись создается автоматически. • SrvAccountUser – учетная запись пользователя задана вручную. В этом случае требуется задать значения параметров SERVERACCOUNTNAME и SERVERACCOUNTPWD.
SERVERACCOUNTNAME	Имя учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser.	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
SERVERACCOUNTPWD	Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser	Строковое значение.
SERVERCER	Длина ключа для сертификата Сервера администрирования (в битах).	• 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит. • Значение не задано – длина ключа для сертификата Сервера администрирования составляет 1 024 бит.
DBTYPE	Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования. Этот параметр является обязательным.	• MySQL – будет использоваться база данных MySQL; в этом случае следует задать значения параметров MYSQLSERVERNAME, MYSQLSERVERPORT,MYSQLDBNAME, MYSQLACCOUNTNAME, MYSQLACCOUNTPWD. • MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express). В этом случае следует задать значения параметров MSSQLSERVERNAME, MSSQLDBNAME, MSSQLAUTHTYPE.
MYSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
MYSQLSERVERPORT	Номер порта для подключения к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.
MYSQLDBNAME	Имя базы данных, которая будет создана для размещения данных Сервера администрирования. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.
MYSQLACCOUNTNAME	Имя учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.
MYSQLACCOUNTPWD	Пароль учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL.	Строковое значение.
MSSQLSERVERNAME	Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.

Имя параметра	Описание параметра	Возможные значения
MSSQLDBNAME	Имя базы данных. Требуется задать значение параметра, если DBTYPE=MySQL	Строковое значение.
MSSQLAUTHTYPE	Тип авторизации при подключении к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MSSQL	• Windows – режим аутентификации Microsoft Windows. • SQLServer – режим аутентификации SQL-сервера. В этом случае требуется задать значения параметров MSSQLACCOUNTNAME и MSSQLACCOUNTPWD.
MSSQLACCOUNTNAME	Имя учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer	Строковое значение.
MSSQLACCOUNTPWD	Пароль учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer	Строковое значение.
CREATE_SHARE_TYPE	Способ задания папки общего доступа.	• Create – создать новую папку общего доступа. В этом случае требуется задать значения параметров SHARELOCALPATH и SHAREFOLDERNAME. • ChooseExisting – выбрать существующую папку. В этом случае требуется задать значение параметра EXISTSHAREFOLDERNAME.

Имя параметра	Описание параметра	Возможные значения
SHARELOCALPATH	Путь к локальной папке. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create	Строковое значение.
SHAREFOLDERNAME	Сетевое имя папки общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create	Строковое значение.
EXISTSHAREFOLDERNAME	Полный путь к существующей папке общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=ChooseExisting	Строковое значение.
SERVERPORT	Номер порта для подключения к Серверу администрирования.	Числовое значение.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.

Имя параметра	Описание параметра	Возможные значения
SERVERADDRESS	Адрес Сервера администрирования.	Строковое значение.
MOBILESERVERADDRESS	Адрес Сервера для подключения мобильных устройств	Строковое значение.

Подробно параметры установки Сервера администрирования описаны в разделе Выборочная установка (на стр. 190).

Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли.

► *Чтобы установить Консоль администрирования на рабочее место администратора, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить только Консоль администрирования Kaspersky Security Center 11** запустите мастер установки Консоли администрирования. Следуйте далее указаниям мастера.

3. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

4. В завершающем окне мастера установки нажмите на кнопку **Запустить**, чтобы начать процесс установки Консоли администрирования.

По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления программ Microsoft Windows.

Изменения в системе после установки Сервера администрирования на устройство

Значок Консоли администрирования

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Найдите его в меню **Пуск** → **Программы** → **Kaspersky Security Center**.

Службы Сервера администрирования и Агента администрирования

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб со свойствами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

Таблица 40. Свойства служб Kaspersky Security Center

Компонент	Имя службы	Отображаемое имя службы	Учетная запись
Сервер администрирования	kladminserver	Сервер администрирования Kaspersky Security Center	Указанная пользователем или специальная, созданная при установке, непривилегированная учетная запись вида KL-AK-*
Агент администрирования	klnagent	Агент администрирования Kaspersky Security Center	Локальная система
Веб-сервер для организации внутреннего портала организации	klwebsrv	Веб-сервер "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер активации	klactprx	Прокси-сервер активации "Лаборатории Касперского"	Специальная непривилегированная учетная запись KlScSvc
Прокси-сервер KSN	ksnproxy	Прокси-сервер Kaspersky Security Network	Специальная непривилегированная учетная запись KlScSvc

Серверная версия Агента администрирования

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его

составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка реализована программно с учетом того, что компоненты установлены на одном компьютере. Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления программами, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство с Сервером администрирования невозможна.

Вы можете просматривать свойства служб Сервера и Агента администрирования, а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала Kaspersky Event Log.

Не рекомендуется вручную запускать и отключать службы и менять учетные записи в настройках служб. При необходимости вы можете поменять учетную запись службы Сервера администрирования с помощью утилиты klsrvswch.

Учетные записи и группы пользователей

По умолчанию инсталлятор Сервера администрирования создает следующие учетные записи:

- - KL-AK-*: учетная запись службы Сервера администрирования;
- - KlScSvc: учетная запись для прочих служб из состава Сервера администрирования;
- - KlPxeUser: учетная запись для развертывания операционных систем.

Если на этапе работы инсталлятора вы выбирали другие учетные записи для службы Сервера администрирования и прочих служб, то будут использованы указанные вами учетные записи.

На устройстве, где установлен Сервер администрирования, также автоматически создаются локальные группы безопасности KLAdmins и KLOperators. Если Сервер администрирования устанавливается на контроллер домена, то автоматически создаются доменные группы безопасности KLAdmins и KLOperators.

При настройке почтовых уведомлений администратору может потребоваться завести учетную запись на почтовом сервере для ESMTP-аутентификации.

См. также:

Учетные записи для работы с СУБД 179

Удаление программы

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы (включая плагины). Если во время работы мастера вы не задали удаление папки общего доступа (Share), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

После удаления программы в системной временной папке могут оставаться файлы.

Мастер удаления программы предложит вам сохранить резервную копию Сервера администрирования.

При удалении программы с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы программы удаления. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление программы.

Обновление предыдущей версии Kaspersky Security Center

Вы можете установить Сервер администрирования версии 11 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 10 Service Pack 1). При обновлении до версии 11 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 11, выполните следующие действия:*

1. Запустите исполняемый файл setup.exe для версии 11.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

   В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center 11** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

   Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **положения и условия настоящего Лицензионного соглашения;**
   - **Политику конфиденциальности, которая описывает обработку данных.**

   Установка программы будет продолжена после установки обоих флажков. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для ранних версий.

   Kaspersky Security Center поддерживает восстановление данных из резервной копии данных Сервера администрирования, сформированной более ранней версией программы.

2. Если требуется создать резервную копию, в открывшемся окне **Создание резервной копии Сервера администрирования** установите флажок **Создать резервную копию Сервера администрирования**.

   Резервная копия данных Сервера администрирования создается при помощи утилиты klbackup. Эта утилита входит в состав дистрибутива программы и располагается в корне папки установки Kaspersky Security Center (см. раздел "Резервное копирование и восстановление данных Сервера администрирования" на стр. 564).

3. Установите Сервер администрирования версии 11, следуя указаниям мастера установки.

   Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности обновляемой версии.

4. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования (см. раздел

"Установка программ с помощью задачи удаленной установки" на стр. 272).

После выполнения задачи удаленной установки версия Агента администрирования будет обновлена.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, обновление других Серверов администрирования в сети можно проводить с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования.

При обновлении Сервера администрирования из более ранней версии все установленные плагины автоматически удаляются. Устанавливаются новые версии этих плагинов.

При обновлении Консоли администрирования из более ранней версии, установленные плагины, поддерживающие обновление, обновляются автоматически. Плагины, которые не поддерживают обновление, автоматически удаляются, затем устанавливаются новые версии этих плагинов.

Первоначальная настройка Kaspersky Security Center

В этом разделе описаны шаги, которые вы должны выполнить после установки Kaspersky Security Center.

В этом разделе

Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Программа Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения системы централизованного управления защитой, с помощью мастера первоначальной настройки. Эта настройка выполняется в мастере первоначальной настройки. В процессе работы мастера вы можете внести в программу следующие изменения:

- Добавить ключи или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN). При разрешении использования KSN мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений

Messenger).

- Настроить параметры обновлений и закрытия уязвимостей программ, установленных на устройствах.
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вирусов, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

> Мастер первоначальной настройки создает политики защиты только для тех программ, для которых они еще не присутствуют в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

В этом разделе

Запуск мастера первоначальной настройки Сервера администрирования

Программа автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► *Чтобы запустить мастер первоначальной настройки вручную, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи → Мастер первоначальной настройки Сервера администрирования**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера.

Шаг 1. Настройка дополнительных компонентов

Укажите, требуется ли вашей организации управление корпоративными мобильными устройствами. Выберите один из следующих вариантов:

- **Не включать Управление мобильными устройствами**

  Выберите этот вариант, если вам не нужны возможности Управления мобильными устройствами.

  При наличии специальной лицензии Управление мобильными устройствами можно включить позже в любое время (см. раздел "Включение Управления мобильными устройствами" на стр. 676).

- **Включить Управления мобильными устройствами**

  Выберите этот вариант, если вы хотите управлять мобильными устройствами сотрудников.

Шаг 2. Выбор способа активации программы

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите код активации

  Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

  Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

- Укажите файл ключа

  Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

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

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

- Отложите активацию программы

  Программа будет работать в режиме Базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования.

Если вы выбрали отложенную активацию программы, вы можете добавить ключ позже в любое время.

► *Чтобы добавить ключ после завершения работы мастера первоначальной настройки, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Нажмите на кнопку **Добавить код активации или ключ**.

   Откроется мастер добавления ключа.
3. Следуйте далее указаниям мастера.

Шаг 3. Настройка параметров прокси-сервера

Настройте параметры доступа Kaspersky Security Center к интернету.

Установите флажок **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если флажок установлен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

  Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

  Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

После того, как вы начали вводить пароль, становится доступна кнопка **Показать**. Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Шаг 4. Проверка обновлений для плагинов и инсталляционных пакетов

Настройте параметры проверки установленных плагинов и инсталляционных пакетов на актуальность. Выберите один из следующих вариантов:

- **Проверить актуальность плагинов и инсталляционных пакетов**

  Запуск проверки на актуальность. Если проверка обнаружит использование устаревших версий плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.

- **Пропустить проверку**

  Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Этот вариант можно выбрать, например, если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить пользоваться устаревшей версией программы.

Пропуск проверки актуальности плагинов и инсталляционных пакетов может привести к некорректной работе программы.

Шаг 5. Настройка Kaspersky Security Network

Прочтите Положение о Kaspersky Security Network (KSN), которое отображается в окне. Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center в автоматическом режиме будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории

Касперского". Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center не будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории Касперского".

Шаг 6. Настройка параметров отправки почтовых уведомлений

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе программ "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках программ.

Для настройки рассылки оповещений о возникающих событиях программ "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **SMTP-серверы**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. В качестве адреса может использоваться IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят, параметры ESMTP-аутентификации недоступны.

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**.

Шаг 7. Настройка параметров управления обновлениями

Настройте параметры работы с обновлениями программ, установленных на клиентских устройствах.

В блоке параметров **Режим поиска и установки обновлений** вы можете выбрать один из режимов поиска

и установки обновлений Kaspersky Security Center:

- **Искать требующиеся для установки обновления**

  Создается задача **Поиск уязвимостей и требуемых обновлений**.

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

  Создаются задачи **Поиск уязвимостей и требуемых обновлений** и **Установка требуемых обновлений и закрытие уязвимостей**.

В блоке параметров **Служба Windows Server Update Services** вы можете выбрать один из способов синхронизации обновлений:

- **Использовать имеющийся в сети WSUS-сервер**

  Задача **Синхронизация обновлений Windows Update** не создается.

  По умолчанию этот вариант выбран.

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Создается задача **Синхронизация обновлений Windows Update**.

Шаг 8. Создание первоначальной конфигурации защиты

В окне **Создание первоначальной конфигурации защиты** отображается список создаваемых политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

Во время создания политик и задач откроется окно первоначальной настройки доверенной зоны Kaspersky Security Center. Программа предложит внести в доверенную зону проверенных "Лабораторией Касперского" поставщиков, чтобы исключить их программы из проверки для предотвращения случайной блокировки. Вы можете создать рекомендованные исключения сейчас или создать список исключений позже, выбрав в дереве консоли **Политики** → меню свойств Kaspersky Endpoint Security → **Продвинутая защита** → **Предотвращение вторжений** → **Настройка** → **Добавить**. Список исключений проверки доступен для редактирования в любой момент дальнейшей работы с программой.

Работа с доверенной зоной выполняется средствами программы Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в онлайн-справке Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.1.0/ru-RU/127971.htm.

Для завершения первоначальной настройки доверенной зоны и возвращения к мастеру нажмите **ОК**.

Нажмите **Далее**. Кнопка станет доступна, когда все необходимые политики и задачи будут созданы.

Шаг 9. Подключение мобильных устройств

Если ранее в параметрах мастера вы включили Управление мобильными устройствами (см. раздел "Шаг 1. Настройка дополнительных компонентов" на стр.215), настройте параметры подключения корпоративных мобильных устройств управляемой организацией. Если вы не включили Управление мобильными устройствами, этот шаг будет пропущен.

► *Чтобы настроить порты подключения мобильных устройств, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить порты**.

   Откроется окно свойств Сервера администрирования на разделе **Дополнительные порты**.
3. В разделе **Дополнительные порты** вы можете настроить параметры подключения мобильных устройств:

   - **SSL-порт для прокси-сервера активации**

     Номер SSL-порта для подключения Kaspersky Endpoint Security для Windows к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17000.

   - **Открыть порт для мобильных устройств**

     Открывается порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

     По умолчанию параметр включен.

   - **Порт для синхронизации мобильных устройств**

     Номер порта, по которому мобильные устройства подключаются к Серверу администрирования и обмениваются с ним информацией. По умолчанию установлен порт 13292.

     Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

   - **Порт для активации мобильных устройств**

     Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17100.

   - **Открыть порт для устройств с защитой на уровне UEFI**

     Устройства с защитой на уровне UEFI могут подключаться к Серверу

администрирования.

- **Порт для устройств с защитой на уровне UEFI**

  Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию установлен порт 13294.

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Вам потребуется настроить аутентификацию Сервера администрирования мобильными устройствами и аутентификацию мобильных устройств Сервером администрирования. Архитектуру программы можно настроить позднее, независимо от мастера первоначальной настройки.

► *Чтобы настроить параметры аутентификации Сервера администрирования мобильными устройствами, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить аутентификацию**.

   Откроется окно свойств Сервера администрирования на разделе **Сертификаты**.
3. Выберите вариант аутентификации для мобильных устройств в блоке параметров **Аутентификация Сервера мобильными устройствами** и для устройств со встроенной защитой на уровне UEFI в блоке параметров **Аутентификация Сервера устройствами с защитой на уровне UEFI**.

   Аутентификация Сервера администрирования при обмене информацией с клиентскими устройствами выполняется на основании сертификата.

   По умолчанию выбрано использование сертификата, созданного при установке Сервера администрирования. При необходимости можно добавить новый сертификат.

► *Чтобы добавить новый сертификат (не обязательно), выполните следующие действия:*

1. Выберите вариант **Другой сертификат**.

   Появится кнопка **Обзор**.
2. Нажмите на кнопку **Обзор**.
3. В появившемся окне настройте параметры сертификата:
   - **Тип сертификата**
   - Срок активации:
     - **Немедленно**

       Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

       Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

- **Через указанный срок (сут)**

  Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

  После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

4. Вы можете нажать на кнопку **Свойства**, чтобы просмотреть параметры выбранного сертификата Сервера администрирования.

► *Чтобы перевыпустить сертификат, выпущенный средствами Сервера администрирования:*

1. Нажмите на кнопку **Перевыпустить**.
2. В открывшемся окне настройте следующие параметры:
   - Адрес подключения:
     - **Оставить адрес подключения прежним**

       Адрес Сервера администрирования, к которому подключаются мобильные устройства, останется прежним.

       По умолчанию этот вариант выбран.

     - **Изменить адрес подключения на**

       Если необходимо, чтобы мобильные устройства подключались по другому адресу, укажите в поле требуемый адрес.

       При изменении адреса подключения мобильных устройств необходимо выпустить новый сертификат. Старый сертификат будет недействительным на подключенных мобильных устройствах. Ранее подключенные устройства не смогут подключиться к Серверу администрирования и перестанут быть управляемыми.

   - Срок активации:
     - **Немедленно**

       Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

       Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

     - **Через указанный срок (сут)**

       Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**.

После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну **Сертификаты**.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

► *Чтобы настроить выпуск, автоматическое обновление и шифрование сертификатов общего типа для идентификации мобильных устройств Сервером администрирования, выполните следующие действия:*

1. Нажмите на кнопку **Настроить** справа от поля **Аутентификация мобильных устройств**.

   Откроется окно **Правила выпуска сертификатов** на разделе **Выпуск мобильных сертификатов**.
2. При необходимости настройте следующие параметры в блоке параметров **Параметры выпуска**:
   - **Срок действия сертификата, дней**

     Срок действия сертификата в днях. По умолчанию срок действия сертификата равен 365 дням. По истечении этого срока мобильное устройство не сможет подключаться к Серверу администрирования.
   - **Источник сертификата**

     Выбор источника сертификатов общего типа для мобильных устройств: сертификаты выпускает Сервер администрирования или сертификаты задаются вручную.

   Вы можете изменить шаблон сертификата, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей. В этом случае будут доступны следующие поля выбора шаблона:

   - **Шаблон по умолчанию**

     Использование сертификата, выпущенного внешним источником сертификатов – центром сертификации – по шаблону, заданному по умолчанию.

     По умолчанию выбран этот вариант.
   - **Другой шаблон**

     Выбор шаблона, на основании которого будут выпускаться сертификаты. Шаблоны сертификатов можно задать в домене. По кнопке **Обновить список** можно обновить список шаблонов сертификатов.
3. При необходимости задайте следующие параметры автоматического выпуска сертификатов в блоке параметров **Параметры автоматического обновления**:
   - **Обновлять, когда до истечения срока действия осталось (сут)**

     Количество дней до истечения срока действия текущего сертификата, за которое Сервер администрирования должен выпустить новый сертификат. Например, если в поле указано значение 4, Сервер администрирования выпустит новый сертификат

за четыре дня до окончания срока действия текущего сертификата. По умолчанию указано значение 7.

- **Автоматически перевыпускать сертификат, если это возможно**

  Сертификаты будут перевыпускаться автоматически, если это возможно. Автоматический перевыпуск недоступен, если сертификат был задан вручную. Если флажок снят, сертификаты автоматически не перевыпускаются. По умолчанию флажок снят.

Сертификаты обновляются автоматически центром сертификации.

4. При необходимости настройте параметры расшифровки сертификатов при установке в блоке параметров **Защита паролем**.

   Установите флажок **Запрашивать пароль при установке сертификата**, чтобы при установке сертификата на мобильное устройство у пользователя запрашивался пароль. Пароль используется только один раз, при установке сертификата на мобильное устройство.

   Пароль будет автоматически сгенерирован средствами Сервера администрирования и отправлен по указанному вами адресу электронной почты. Вы можете указать адрес электронной почты пользователя либо свой собственный, если хотите затем передать пользователю пароль другим способом.

   Вы можете указать количество символов пароля для расшифровки сертификата с помощью ползунка.

   Функция запроса пароля необходима, например, для защиты общего сертификата в автономном пакете установки Kaspersky Endpoint Security для Android. Защита паролем не позволит злоумышленнику получить доступ к общему сертификату при краже автономного пакета установки с Веб-сервера Kaspersky Security Center.

   Если флажок снят, расшифровка сертификата при установке будет проводиться автоматически и у пользователя не будет запрашиваться пароль. По умолчанию флажок снят.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну мастера первоначальной настройки.

   Нажмите на кнопку **Отмена**, чтобы вернуться к мастеру первоначальной настройки без сохранения внесенных изменений.

► *Чтобы включить функцию перемещения мобильных устройств в нужную вам группу администрирования,*

в поле **Автоматически перемещать мобильные устройства** установите флажок **Создать правило перемещения мобильных устройств**.

Если флажок **Создать правило перемещения мобильных устройств** установлен, программа автоматически создает правило перемещения, которое перемещает устройства под управлением операционных систем Android и iOS в группу **Управляемые устройства**.

- с операционными системами Android , на которых установлен Kaspersky Endpoint Security для Android и мобильный сертификат.

- с операционными системами iOS, на которых установлен Kaspersky Safe Browser и мобильный сертификат.

Если такое правило уже существует, то программа не создает правило.

По умолчанию флажок снят.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser. Соответствующие функции Kaspersky Security Center могут работать некорректно.

Шаг 10. Обнаружение устройств

В информационном окне **Обнаружение устройств** отображается информация о статусе опроса сети Сервером администрирования.

Вы можете просмотреть обнаруженные в сети Сервером администрирования устройства и получить справку по работе с окном **Обнаружение устройств** по ссылкам в нижней части окна.

Шаг 11. Завершение работы мастера первоначальной настройки

В окне завершения работы мастера первоначальной настройки установите флажок **Запустить мастер удаленной установки**, если вы хотите запустить автоматическую установку антивирусных программ и / или Агента администрирования на устройства в вашей сети.

Для завершения работы мастера нажмите на кнопку **Готово**.

Настройка подключения Консоли администрирования к Серверу администрирования

В предыдущих версиях Kaspersky Security Center Консоль администрирования подключалась к Серверу администрирования, используя SSL-порт TCP 13291, а также SSL-порт TCP 13000. Начиная с версии Kaspersky Security Center 10 Service Pack 2, SSL-порты, используемые программой, строго разделены, и использование портов не по назначению невозможно:

- SSL-порт TCP 13291 могут использовать только Консоль администрирования и объекты автоматизации утилиты klakaut.
- SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования),
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

► *Чтобы разрешить подключение Консоли администрирования по порту 13000, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 1.
4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

Настройка профилей соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows.

Использование различных адресов одного и того же Сервера администрирования

Описанное ниже применимо только для Kaspersky Security Center 10 Service Pack 1 и выше.

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Сеть**, вложенный раздел **Подключение**). В окне создания профиля необходимо снять флажок **Использовать только для получения обновлений** и установить флажок **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне (на стр. 85)), в профиле подключения следует указать адрес шлюза соединений в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Описанное ниже применимо только для Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 и выше.

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и установить либо снять флажок **Использовать только для получения обновлений**:

- установить флажок, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- снять флажок, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится

истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

См. также:

Шифрование подключения SSL/TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием SSL/TLS. Вы можете включить SSL/TLS для Сервера администрирования и Сервера iOS MDM. Kaspersky Security Center поддерживает SSL v3, также как и Transport Layer Security (TLS v1.0, 1.1, и 1.2). Вы можете выбрать протокол шифрования и наборы шифрования. Kaspersky Security Center использует самоподписанные сертификаты. Дополнительная настройка для iOS устройств не требуется. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные аккредитованным центром сертификации.

Сервер администрирования

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования, выполните следующие действия:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер администрирования (например, локально с помощью команды regedit в меню Пуск → Выполнить).
2. Перейдите в раздел:
   - для 64-разрядной системы:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\Transport`

   - для 32-разрядной системы:

     `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\Transport`
3. Создайте ключ с именем `SrvUseStrictSslSettings`.
4. Укажите тип ключа `DWORD`.
5. Установите значение ключа:
   - `0` – все разрешенные протоколы шифрования и наборы шифрования включены.
   - `1` – SSL v2 выключен.

Наборы шифрования:

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- IDEA-CBC-SHA
- RC4-SHA
- RC4-MD5
- DES-CBC3-SHA

- 2 – SSL v2 и SSL v3 выключены (значение указано по умолчанию).

  Наборы шифрования:

  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - SEED-SHA
  - CAMELLIA128-SHA
  - IDEA-CBC-SHA
  - RC4-SHA
  - RC4-MD5
  - DES-CBC3-SHA

- 3 – только TLS v1.2.

  Наборы шифрования:

- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA128-SHA

6. Перезапустите службу Сервера администрирования Kaspersky Security Center 11.

Сервер iOS MDM

Соединение между iOS устройствами и Сервером iOS MDM зашифровано.

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере iOS MDM, выполните следующие действия:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню Пуск → Выполнить.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset`

   - для 32-разрядной системы:

     `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset`
3. Создайте ключ с именем `StrictSslSettings`.
4. Укажите тип ключа `DWORD`.
5. Установите значение ключа:
   - `2` – без ограничений (разрешены TLS 1.0, TLS 1.1, TLS 1.2)
   - `3` – только TLS 1.2 (значение указано по умолчанию)
6. Перезапустите службу Сервера iOS MDM Kaspersky Security Center 11.

Уведомления о событиях

В этом разделе описано, как выбрать способ уведомления администратора о событиях на клиентских устройствах, а также как настроить параметры уведомления о событиях.

Кроме того, описано, как проверить распространение уведомлений о событиях с помощью тестового "вируса" Eicar.

В этом разделе

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений.

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. 234).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   В результате откроется окно **Свойства: События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

- **Электронная почта**

На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. В качестве адреса можно использовать IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры уведомлений (например, указать тему сообщения).

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильность настройки сообщений: программа отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. В качестве адреса можно использовать IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры

уведомлений (например, указать тему сообщения).

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

  По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   > Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

   Программа отправляет тестовое уведомление указанному получателю.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. раздел "Общие параметры политик" на стр. 623) или параметров программы (см. раздел "Выбор событий для программы" на стр. 751).

См. также:

Обработка и хранение событий на Сервере администрирования.....557

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

► *Чтобы проверить распространение уведомлений о событиях, выполните следующие действия:*

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Снова включите задачу постоянной защиты файловой системы.
2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

   В рабочей области узла **Сервер администрирования** на закладке **События** в выборке **Последние события** отобразится запись об обнаружении "вируса".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство программ безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR http://www.eicar.org.

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

Таблица 41. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Доменная
%EVENT%	Событие
%DESCR%	Описание события
%RISE_TIME%	Время возникновения
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Имя задачи
%KL_PRODUCT%	Агент администрирования Kaspersky Security Center
%KL_VERSION%	Номер версии Агента администрирования
%HOST_IP%	IP-адрес
%HOST_CONN_IP%	IP-адрес соединения

Пример

Для уведомления о событии используется исполняемый файл (например, *script1.bat)*, внутри которого запускается другой исполняемый файл (например, *script2.bat*) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл *script1.bat*, который, в свою очередь, запустит файл *script2.bat* с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Обнаружение устройств в сети

В этом разделе описаны шаги, которые вы должны выполнить после установки Kaspersky Security Center.

В этом разделе

Сценарий: Обнаружение устройств в сети

Вы должны выполнить поиск устройств перед установкой программ безопасности. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

Обнаружение сетевых устройств содержит следующие этапы:

a. **Первоначальное обнаружение устройств**

   Во время работы Мастера первоначальной настройки программы выполняется первоначальное обнаружение устройств (см. раздел "Шаг 10. Обнаружение устройств" на стр. 225), в результате чего обнаруживаются сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную (см. раздел "Обнаружение устройств" на стр. 238).

b. **Настройка будущих опросов**

   Определите, какой тип обнаружения устройств вы хотите регулярно использовать (см. раздел "Обнаружение устройств" на стр. 238). Убедитесь, что этот тип включен и что расписание опроса соответствует требованиям вашей организации. При настройке расписания опроса опирайтесь на рекомендации для частоты опросов сети (см. раздел "Частота обнаружения устройств" на стр. 933).

c. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. При необходимости можно настроить правила автоматического перемещения этих устройств(см. раздел "Правила перемещения устройств" на стр. 349) в группу **Управляемые устройства**. Можно также настроить правила хранения (см. раздел "Настройка правил хранения для нераспределенных устройств" на стр. 246).

Если вы пропустили шаг, на котором задаются правила, все новые обнаруженные устройства будут помещены в группу **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Результаты

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

См. также:

Порты, используемые Kaspersky Security Center 56

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Основные понятия 33

Архитектура программы 48

Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

В этом разделе

Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Опрос сети Windows**. Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удаться обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.
- **Опрос Active Directory**. Сервер администрирования получает информацию о структуре групп Active Directory, а также информацию о DNS-именах устройств, входящих в группы Active Directory. По умолчанию этот тип опроса включен. При использовании Active Directory рекомендуется использовать опрос Active Directory. В противном случае Сервер администрирования не сможет обнаружить устройства. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.
- **Опрос IP-диапазонов**. Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows или опрос Active Directory.

Если вы настроили и включили правила перемещения устройств (на стр. 349), новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес Active Directory или только определенный домен.

См. также:

Частота обнаружения устройств 933

В этом разделе

Опрос сети Windows

Об опросе сети Windows

При быстром опросе Сервер получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- имя операционной системы;
- IP-адрес
- DNS-имя;
- NetBIOS-имя.

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

► *Чтобы изменить параметры опроса сети Windows, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

   В рабочей области подпапки **Домены** отображается список устройств.

2. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно свойств домена. При необходимости настройте параметры опроса сети Windows:

   - **Включить опрос сети Windows**

     По умолчанию этот вариант выбран. Если не требуется выполнять опрос сети Windows (например, если достаточно опроса Active Directory), можно отменить выбор данного параметра.

   - **Настроить период быстрого опроса**

     По умолчанию интервал времени составляет 15 минут.

     При быстром опросе Сервер получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети.

     Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждый N день**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

     - **N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

     По умолчанию опрос запускается каждые 30 минут, начиная с текущего системного времени.

     - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

     По умолчанию опрос запускается каждую пятницу в 18:00:00.

     - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное

время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

- **Настроить период полного опроса**

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждый N день**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

По умолчанию опрос запускается каждые 30 минут, начиная с текущего системного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию опрос запускается каждую пятницу в 18:00:00.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на

которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Будут запущены оба типа опроса.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса сети Windows осуществляется в окне свойств точки распространения, в разделе **Обнаружение устройств**.

См. также:

Работа с доменами Windows. Просмотр и изменение параметров домена 246

Опрос Active Directory

Используйте опрос Active Directory, если вы используете Active Directory; в противном случае рекомендуется использовать другие типы опросов. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

Просмотр и изменение параметров опроса Active Directory

► *Чтобы просмотреть и изменить параметры опроса групп Active Directory, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.

   Также вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. Нажмите на кнопку **Настроить параметры опроса**.

   В результате откроется окно свойств Active Directory. При необходимости настройте параметры опроса групп Active Directory:

   - **Разрешить опрос Active Directory**

     По умолчанию этот вариант выбран. Однако если Active Directory не используется, в

результаты опроса ничего найдено не будет. В этом случае можно отменить выбор данного параметра.

- **Задать расписание опроса сети**

  По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

  Доступны следующие варианты расписания опроса сети:

  - **Каждый N день**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

  - **N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

  По умолчанию опрос запускается каждые 30 минут, начиная с текущего системного времени.

  - **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию опрос запускается каждую пятницу в 18:00:00.

  - **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

  - **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

- **Дополнительно**

  Можно выбрать домены Active Directory для опроса:

- Домен Active Directory, к которому относится Kaspersky Security Center.
- Лес доменов, к которому относится Kaspersky Security Center.
- Указанный список доменов Active Directory.

  При выборе этого параметра можно добавлять домены в область опроса:

  - Нажмите на кнопку **Добавить**.
  - В соответствующих полях укажите адрес доменного контроллера, а также имя и пароль учетной записи для доступа к нему.
  - Нажмите на кнопку **ОК**, чтобы сохранить изменения.

  Можно выбрать адрес доменного контроллера в списке и нажать на кнопку **Изменить** или **Удалить**, чтобы изменить или удалить его.
- Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса групп Active Directory осуществляются в окне свойств (см. раздел "Параметры политики Агента администрирования" на стр. 624) точки распространения, в разделе **Обнаружение устройств**.

Опрос IP-диапазонов

Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows или опрос Active Directory.

Просмотр и изменение параметров опроса IP-диапазонов

► *Чтобы просмотреть и изменить параметры опроса групп IP-диапазона, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.
2. Если вы хотите, в подпапке **IP-диапазоны** нажмите на кнопку **Добавить подсеть**, чтобы добавить IP-диапазон (см. раздел "Работа с IP-диапазонами" на стр. 247) для опроса, а затем нажмите **ОК**.
3. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно свойств IP-диапазонов. Если требуется, можно поменять параметры опроса IP-диапазонов:

   - **Разрешить опрос IP-диапазонов**

     По умолчанию этот вариант не выбран. Не рекомендуется использовать этот тип

опроса, если вы используете опрос сети Windows или опрос Active Directory.

- **Задать расписание опроса сети**

  По умолчанию интервал времени составляет 420 минут. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

  Доступны следующие варианты расписания опроса сети:

  - **Каждый N день**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

  - **N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

  По умолчанию опрос запускается каждые 30 минут, начиная с текущего системного времени.

  - **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию опрос запускается каждую пятницу в 18:00:00.

  - **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

  - **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Эта кнопка доступна, только если выбран параметр **Разрешить опрос IP-диапазонов**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса IP-диапазонов осуществляются в окне свойств (см. раздел "Параметры политики Агента администрирования" на стр. 624) точки распространения, в разделе **Обнаружение устройств**. Клиентские устройства, найденные в результате опроса IP-диапазонов, отображаются в папке **Домены** виртуального Сервера.

Работа с доменами Windows. Просмотр и изменение параметров домена

► *Чтобы изменить параметры домена, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.
2. Выберите домен и откройте окно его свойств одним из следующих способов:
   - В контекстном меню домена выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

Откроется окно **Свойства: <Имя домена>** можно настроить параметры выбранного домена.

Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Дополнительно** → **Обнаружение устройств** → **Домены**. Папка **Домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, которые были обнаружены во время опроса сети. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров опроса сети и работают, даже если опрос сети выключен.

► *Чтобы настроить правила хранения нераспределенных устройств, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выполните одно из следующих действий:
   - Чтобы настроить параметры родительской группы, в контекстном меню папки **Домены** выберите пункт **Свойства**.

     Откроется окно свойств родительской группы.
   - Чтобы настроить параметры дочерней группы, в контекстном меню дочерней группы выберите пункт **Свойства**.

     Откроется окно свойств дочерней группы.

2. В разделе **Устройства** укажите следующие параметры:

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Наследовать из родительской группы**

     Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

     Этот параметр доступен только для дочерних групп.

     По умолчанию параметр включен.

   - **Форсировать наследование для дочерних групп**

     Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

     По умолчанию параметр выключен.

Ваши изменения сохранены и применены.

Работа с IP-диапазонами

Вы можете настраивать параметры существующих IP-диапазонов, а также создавать новые IP-диапазоны.

В этом разделе

Создание IP-диапазона

► *Чтобы создать IP-диапазон, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. В контекстном меню папки выберите пункт **Новый → IP-диапазон**.

3. В открывшемся окне **Новый IP-диапазон** настройте параметры создаваемого IP-диапазона.

В результате созданный IP-диапазон появится в составе папки **IP-диапазоны**.

Просмотр и изменение параметров IP-диапазона

► *Чтобы изменить параметры IP-диапазона, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. Выберите IP-диапазон и откройте окно его свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

Откроется окно **Свойства: <Название IP-диапазона>** можно настроить параметры выбранного IP-диапазона.

Работа с группами Active Directory. Просмотр и изменение параметров группы

► *Чтобы изменить параметры группы Active Directory, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.
2. Выберите группу Active Directory и откройте окно ее свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

Откроется окно **Свойства: <Название группы Active Directory>** можно настроить параметры выбранной группы Active Directory.

Создание правил автоматического перемещения устройств в группы администрирования

Вы можете настроить автоматическое перемещение устройств, обнаруживаемых при опросе сети организации, в группы администрирования.

► *Чтобы настроить правила автоматического перемещения устройств в группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В рабочей области папки нажмите на кнопку **Настроить правила**.

В результате откроется окно **Свойства: События**. Настройте правила автоматического перемещения устройств в группы администрирования в разделе **Перемещение устройств**.

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли администрирования.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI (см. раздел "Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования" на стр. 249) в свойствах инсталляционного пакета Агента администрирования (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. 143), который будет установлен на временной виртуальной машине (только для Windows).

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

В этом разделе

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

Использование динамического режима для Virtual Desktop Infrastructure (VDI) доступно только для устройств под управлением Windows.

► *Чтобы включить динамический режим VDI, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства: Агент администрирования Kaspersky Security Center**.

3. В окне **Свойства: Агент администрирования Kaspersky Security Center** выберите раздел **Дополнительно**.

4. В разделе **Дополнительно** установите флажок **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

Поиск устройств, являющихся частью VDI

► *Чтобы найти устройства, являющиеся частью VDI, выполните следующие действия:*

1. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
2. В окне **Поиск** на закладке **Виртуальные машины** в раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.
3. Нажмите на кнопку **Найти**.

Будет выполнен поиск устройств, являющихся частью Virtual Desktop Infrastructure.

Перемещение в группу администрирования устройств, являющихся частью VDI

► *Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования, выполните следующие действия:*

1. В рабочей области папки **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   В результате откроется окно свойств папки **Нераспределенные устройства**.

2. В окне свойств папки **Нераспределенные устройства** в разделе **Перемещение устройств** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.

3. В окне **Новое правило** выберите раздел **Виртуальные машины**.
4. В раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.

Будет создано правило перемещения устройств в группу администрирования.

Инвентаризация оборудования, обнаруженного в сети

Kaspersky Security Center получает информацию об оборудовании, найденном в результате обнаружения устройств. Инвентаризации подвергается любое оборудование, подключенное к сети организации. При каждом последующем обнаружении устройств информация об оборудовании обновляется. В списке обнаруженного оборудования могут присутствовать следующие типы устройств:

- устройства;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;
- VoIP-телефоны;
- сетевые хранилища.

Найденное при обнаружении устройств оборудование отображается в папке **Хранилища**, вложенной в папку **Оборудование** дерева консоли.

Администратор может добавлять новые устройства в список оборудования вручную или редактировать информацию об уже имеющемся в сети оборудовании. В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

Администратор может присваивать обнаруженным устройствам признак "Корпоративное оборудование". Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак "Корпоративное оборудование" присваивается по типу устройства. По признаку "Корпоративное оборудование" можно разрешать или запрещать подключение оборудования к сети.

Kaspersky Security Center позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо установить флажок **Устройство списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Networks*.

В этом разделе

Добавление информации о новых устройствах

► *Чтобы добавить информацию о новых устройствах в сети, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** по кнопке **Добавить устройство** откройте окно **Новое устройство**.

   Откроется окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.

   Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:

   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак "Корпоративное". По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Устройство списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области папки **Оборудование**.

Настройка критериев определения корпоративных устройств

► *Чтобы настроить критерии определения корпоративных устройств, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить критерии определения корпоративных устройств**.

   Откроется окно свойств оборудования.
3. В окне свойств оборудования в разделе **Корпоративные устройства** выберите способ присвоения устройству признака "Корпоративное":

   - **Вручную устанавливать для устройства признак "Корпоративное"**. Признак "Корпоративное оборудование" назначается устройству вручную в окне свойств устройства в разделе **Общие**.
   - **Автоматически устанавливать для устройства признак "Корпоративное"**. В блоке параметров **По типу устройства** укажите типы устройств, которым программа будет автоматически присваивать признак "Корпоративное".

4. Нажмите на кнопку **Применить**.

Настройка пользовательских полей

► *Чтобы настроить пользовательские поля устройств, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить пользовательские поля данных**.

   Откроется окно свойств оборудования.
3. В окне свойств оборудования в разделе **Пользовательские поля** нажмите на кнопку **Добавить**.

   Откроется окно **Добавить поле**.
4. В окне **Добавить поле** укажите название пользовательского поля, которое будет отображаться в свойствах оборудования.

   Вы можете создать несколько пользовательских полей с уникальными именами.
5. Нажмите на кнопку **Применить**.

В результате в свойствах оборудования в разделе **Пользовательские поля** будут отображаться добавленные пользовательские поля. Вы можете использовать пользовательские поля для указания специфической информации об устройствах. Например, номер внутренней заявки на приобретение оборудования.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center 11.

В этом разделе

См. также:

О Лицензионном соглашении

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 Kaspersky Security Center.
- Прочитав документ license.txt, включенный в комплект поставки Kaspersky Security Center.
- Прочитав документ license.txt в папке установки Kaspersky Security Center.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

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:

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

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security Center прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

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

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Security Center). Чтобы продолжить использование Kaspersky Security Center в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

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

активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

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*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

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 при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

Варианты лицензирования Kaspersky Security Center

В Kaspersky Security Center лицензия может распространяться на разные группы функциональности.

Базовая функциональность Консоли администрирования

Доступны следующие функции:

- создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов;
- формирование иерархии групп администрирования для управления набором устройств как единым целым;
- контроль состояния антивирусной безопасности организации;
- удаленная установка программ;
- просмотр списка образов операционных систем, доступных для удаленной установки;
- централизованная настройка параметров программ, установленных на клиентских устройствах;
- просмотр и изменение существующих групп лицензионных программ;
- получение статистики и отчетов о работе программ, а также уведомлений о критических событиях;
- управление процессом шифрования и защиты данных;
- просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети;
- централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена;
- управление ролями пользователей.

Программа Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе программ "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования (см. раздел "Об ограничениях базовой функциональности" на стр. 259).

Системное администрирование

Доступны следующие функции:

- удаленная установка операционных систем;
- удаленная установка обновлений программного обеспечения, поиск и закрытие уязвимостей;
- инвентаризация оборудования;
- управление группами лицензионных программ;
- удаленное разрешение подключения к клиентским устройствам с помощью компонента Microsoft®

Windows® "Подключение к удаленному рабочему столу";

- удаленное подключение к клиентским устройствам с помощью совместного доступа к рабочему столу Windows;

Единицей управления для Системного администрирования является клиентское устройство в группе "Управляемые устройства".

С использованием возможности Системного администрирования при инвентаризации доступны подробные сведения об оборудовании устройств.

Для правильной работы Системного администрирования объем свободного места на жестком диске должен составлять не менее 100 ГБ.

Управление мобильными устройствами

Возможность Управления мобильными устройствами предназначена для управления мобильными устройствами Exchange ActiveSync и iOS MDM.

Для мобильных устройств Exchange ActiveSync доступны следующие функции:

- создание и редактирование профилей управления мобильными устройствами, назначение профилей почтовым ящикам пользователей;
- настройка параметров работы мобильного устройства (синхронизация почты, использование приложений, пароль пользователя, шифрование данных, подключение съемных дисков);
- установка сертификатов на мобильные устройства.

Для iOS MDM-устройств доступны следующие функции:

- создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства;
- установка приложений на мобильное устройство через App Store® или с помощью манифест-файлов (.plist);
- возможность блокировать мобильное устройство, сбрасывать пароль мобильного устройства и удалять все данные с мобильного устройства.

С использованием возможности Управление мобильными устройствами доступно выполнение команд, предусмотренных соответствующими протоколами.

Единицей управления для Управления мобильными устройствами является мобильное устройство. Мобильное устройство считается управляемым, как только оно подключается к Серверу мобильных устройств.

Об ограничениях базовой функциональности

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования. Далее приведено описание ограничений, которые накладываются на работу программы в этом режиме.

Управление мобильными устройствами

Невозможно создать новый профиль и назначить его мобильному устройству (iOS MDM) или почтовому ящику (Exchange ActiveSync). Изменение существующих профилей и их назначение почтовым ящикам доступно всегда.

Управление программами

Невозможно запустить задачи установки и удаления обновлений. Все задачи, запущенные до истечения срока действия лицензии, выполняются до конца, но последние обновления не устанавливаются. Например, если до истечения срока действия лицензии была запущена задача установки критических обновлений, то будут установлены только критические обновления, найденные до истечения срока действия лицензии.

Запуск и редактирование задач синхронизации, поиска уязвимостей и обновления базы уязвимостей доступны всегда. Ограничения также не накладываются на просмотр, поиск и сортировку записей в списке уязвимостей и обновлений.

Дистанционная установка операционных систем и программ

Невозможно запустить задачи снятия и установки образа операционной системы. Задачи, запущенные до истечения срока действия лицензии, выполняются до конца.

Инвентаризация оборудования

Недоступно получение информации о новых устройствах с помощью Сервера мобильных устройств. При этом информация о компьютерах и подключаемых устройствах обновляется.

Не работают оповещения об изменении конфигурации устройств.

Список оборудования доступен для просмотра и редактирования вручную.

Управление группами лицензионных программ

Невозможно добавить новый ключ.

Не рассылаются оповещения о том, что превышены ограничения на использование ключей.

Удаленное подключение к клиентским устройствам

Удаленное подключение к клиентским устройствам недоступно.

Антивирусная безопасность

Антивирус использует базы, установленные до истечения срока действия лицензии.

Интеграция с облачными окружениями (Amazon Web Services, Microsoft Azure)

При работе в облачном окружении вы не можете использовать инструменты AWS API или Azure API для опроса облачных сегментов и установки программ на устройства. Недоступны также элементы интерфейса, отображающие функции, специфические для работы в облачном окружении.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если программа была активирована с помощью кода активации, в некоторых случаях после активации программа регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа. Для отправки запросов необходимо предоставить программе доступ в интернет.

Если код активации был потерян после активации программы, вы можете восстановить его. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 939).

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

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

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 веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/en/) на основе имеющегося кода активации.

О предоставлении данных

При установке данного программного обеспечения, правообладателем которого является АО "Лаборатории Касперского" (далее также Правообладатель), вы соглашаетесь автоматически предоставлять указанную ниже информацию Правообладателю с целью повышения уровня защиты, содействия при подготовке наиболее подходящих и информативных коммерческих предложений, а также для получения данных о распространении программного обеспечения по всему миру, для улучшения качества работы программного обеспечения, для быстрой идентификации и исправления ошибок, связанных с установкой продукта, а также для оценки количества пользователей.

Для идентификации и управления устройствами и мобильными устройствами, подключенными к Серверу администрирования Kaspersky Security Center, некоторые из перечисленных ниже данных также обрабатываются локально в Kaspersky Security Center.

Данные, передаваемые Правообладателю

При использовании KSN Правообладатель будет получать и обрабатывать следующие данные в автоматическом режиме (использование службы KSN не является обязательным и эти данные предоставляются, только если вы согласились использовать KSN):

- информацию о версии установленной на Компьютере операционной системы (ОС) и установленных пакетах обновлений, разрядность, редакцию и параметры режима работы ОС;
- информацию о ПО Правообладателя: тип ПО, полную версию ПО, локализацию, уникальный идентификатор установки ПО, данные об установленных обновлениях ПО, статус работы используемого ПО, версии установленных компонентов ПО и статус их работы, а также значение фильтра TARGET и версию используемого протокола соединения с сервисами Правообладателя;
- информацию об уникальном идентификаторе Компьютера, на котором установлено ПО;
- IP-адрес и порт Компьютера, с которого осуществляется соединение с сервисами Правообладателя;
- информацию о дате и времени индексного файла, загруженного в результате последнего обновления и загружаемого в текущем обновлении, идентификаторы и метки времени компонентов обновлений, загруженных в результате последнего обновления и загружаемых в текущем обновлении, идентификатор категории ошибки, возникшей при обновлении, наименование компонента обновления;
- информацию о версии компонента обновления ПО, количество аварийных завершений работы компонента обновления ПО при выполнении задач обновления за время работы компонента, идентификатор типа задачи обновления, состояние ПО после завершения задачи обновления, количество неуспешных завершений задач обновления компонента обновления ПО, код результата обновления;
- название, версию, используемый язык программного продукта, для которого устанавливается обновление;
- версию базы данных обновлений, используемой программным обеспечением при установке;
- результат установки обновления;
- параметры ПО, используемые при установке обновлений: идентификаторы выполненных

операций, коды результатов выполнения операций;

- тип платформы Managed Services Providers, версия приложения Правообладателя, которое используется для интеграции ПО с платформой Managed Services Providers.

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- тип, версию и локализацию установленного ПО;
- версии установленных Обновлений ПО;
- идентификатор Компьютера и идентификатор установки ПО на Компьютере;
- код активации и уникальный идентификатор активации текущей лицензии;
- тип, версию и разрядность операционной системы.

Если получение Обновлений выполняется с серверов обновлений Правообладателя, то для целей улучшения качества работы механизма обновления Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- тип и версию установленного ПО;
- идентификатор сессии обновления;
- уникальный идентификатор действующей лицензии;
- уникальный идентификатор установки ПО на компьютере.

Данные, обрабатываемые локально

Kaspersky Security Center предназначен для идентификации и управления устройствами (физическими или виртуальными) и мобильными устройствами, подключенными к Серверу администрирования Kaspersky Security Center с помощью специальных программных средств. В связи с этим, Kaspersky Security Center может принимать, хранить и обрабатывать следующие типы данных:

- Настройки управляемых программ и компонентов Kaspersky Security Center (представленные в виде политик и профилей политик).
- Журнал событий Kaspersky Event Log для управляемых программ и компонентов Kaspersky Security Center.
- Управляемые устройства и устройства, обнаруженные в сети организации (физические и виртуальные):
    - Для Windows:
        - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: имя и описание устройства, домен, имя устройства в среде Windows, DNS-имя и IP-адрес, имя производителя операционной системы, папка расположения операционной системы, является ли устройство виртуальной машиной и тип гипервизора.
        - Прочие характеристики управляемых устройств и их компонентов, например, состояние

агента обновлений Windows и разрядность операционной системы.

- Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидание перезапуска, время включения устройства и атрибут “Видимый”.
- Данные об учетных записях пользователей устройств и их сеансах работы.

- Для Linux:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: имя и описание устройства, домен, DNS-имя, IP-адрес и операционная система.
  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидание перезапуска, время включения устройства и атрибут “Видимый”.
- Для macOS:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: имя и описание устройства, домен, IP-адрес, название и имя производителя операционной системы.
  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидание перезапуска, время включения устройства и атрибут “Видимый”.
- Для виртуальных машин:
  - Тип виртуальной машины.

- Данные о мобильных устройствах, передаваемые по протоколу Exchange ActiveSync:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название операционной системы, номер IMEI и номер телефона.
  - Характеристики управляемого устройства и его компонентов: статус управления устройством, поддержка SMS, разрешение на отправку SMS-сообщений, поддержка GCM, поддержка пользовательских команд, папка хранения операционной системы и имя устройства.
  - Данные об установленных на устройстве приложениях "Лаборатории Касперского": название и версия приложения, дата установки приложения, текущее состояние, дата и время последнего обновления, список установленных обновлений, дата и время выпуска баз приложения, количество записей в базе данных, теги и комментарии, добавленные администратором, резервные копии ключей шифрования для функции контейнеризации приложения, одноразовые пароли разблокировки и параметры приложения.
  - Данные о действиях на управляемых устройствах: местоположение устройства (при использовании команды Определить местоположение), время последней синхронизации, время последнего подключения к Серверу администрирования и данные о поддержке синхронизации.

- События, связанные с работой задач, инициированных компонентами приложений "Лаборатории Касперского": изменение текущего статуса приложения "Лаборатории Касперского" или самого устройства, изменение параметров приложений "Лаборатории Касперского" на устройстве.

- Данные о мобильных устройствах, передаваемые по протоколу iOS MDM:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название и номер сборки операционной системы, номер модели устройства, номер IMEI, UDID, MEID, серийный номер, объем памяти, версия прошивки модема, MAC-адрес Bluetooth, MAC-адрес Wi-Fi и данные SIM-карты (код ICCID как часть идентификатора SIM-карты).
  - Данные о мобильной сети, используемой мобильным устройством: тип мобильной сети, название используемой мобильной сети, название домашней мобильной сети, версия параметров оператора мобильной сети, статус голосового роуминга и роуминга данных, код страны для домашней сети, код страны пребывания, код страны используемой сети и уровень шифрования.
  - Параметры безопасности управляемого устройства: использование пароля и его соответствие параметрам политики, список конфигурационных профилей и provisioning-профилей, используемых для установки сторонних приложений.
  - Дата последней синхронизации с Сервером администрирования и статус управления устройством.
- Данные о программах "Лаборатории Касперского", установленных на устройстве:
  - Управляемые программы и компоненты Kaspersky Security Center, установленные на устройстве.
  - Параметры программ "Лаборатории Касперского", установленных на управляемом устройстве: статус и версия программы "Лаборатории Касперского", поддерживается ли постоянное соединение с Сервером администрирования, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, задачи для программы безопасности "Лаборатории Касперского", наличие и статус компонентов программного решения, версия антивирусных баз и данные о параметрах программы "Лаборатории Касперского".
  - Статистика работы программы: события, связанные с изменениями статуса компонентов программы "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных программными компонентами.
  - Состояние устройства, определенное программой "Лаборатории Касперского".
- Список управляемых программируемых логических контроллеров (ПЛК).
- Данные, обрабатываемые функцией Системное администрирование:
  - Данные о программах, установленных на управляемых устройствах.
  - Данные об обновлениях, доступных для Microsoft Windows и сторонних программ, установленных на управляемых устройствах.
  - Данные об уязвимостях программного обеспечения, обнаруженных на управляемых

устройствах.

- Реестр оборудования, обнаруженного на управляемых устройствах.

- Список исполняемых файлов, обнаруженных на управляемых устройствах функцией Контроль программ.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center.
- Данные о файлах, находящихся на Карантине (не сами файлы).
- Резервная копия – данные о файлах, измененных или удаленных в процессе лечения (не сами файлы).
- Данные о файлах, лечение которых было отложено (не сами файлы).
- Учетные записи пользователей (имена и пароли пользователей).
- Параметры шифрования Kaspersky Endpoint Security для Windows (хранилище ключей шифрования, статус шифрования устройств).
- Пользовательские категории программ.
- Данные о лицензировании и активации программ.

Перечисленные выше данные либо сохраняются в базу данных Сервера администрирования администратором с помощью Консоли администрирования, либо попадают в Агент администрирования или программу безопасности, а затем передаются на Сервер администрирования. Агент администрирования может хранить эти данные до передачи на Сервер администрирования.

Данные хранятся в базе данных Сервера администрирования. Имена пользователей и пароли хранятся в зашифрованном виде.

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только посредством файлов дампа или файлов трассировки Kaspersky Security Center.

Файлы дампа или файлы трассировки Kaspersky Security Center содержат случайные данные Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера iOS MDM, Сервера мобильных устройств Exchange ActiveSync и Kaspersky Security Center System Health Validator; эти файлы могут содержать персональные данные. Файлы дампа и файлы трассировки хранятся в открытой форме на устройстве, на котором установлен Сервер администрирования. Файлы дампа и файлы трассировки не передаются в "Лабораторию Касперского" автоматически; однако администратор может передать эти данные в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное

время.

О подписке

Подписка на Kaspersky Security Center – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании программы по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Вы можете продлить подписку на веб-сайте поставщика услуг.

События превышения лицензионного ограничения

Kaspersky Security Center позволяет получать информацию о событиях превышения лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90%–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100%–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

См. также:

Настройка общих параметров Сервера администрирования 556

Особенности лицензирования Kaspersky Security Center и управляемых программ

Лицензирование Сервера администрирования и управляемых программ имеет следующие особенности:

- На Сервер администрирования можно добавить только один активный ключ или действительный код активации(см. раздел "Программы "Лаборатории Касперского": лицензирование и активация" на стр. 295) для активации возможностей Системного администрирования, Управления мобильными устройствами или интеграции с SIEM-системами. Подробную информацию о возможностях Kaspersky Security Center, которые доступны для различных активных ключей или действительных кодов активации, добавленных на Сервер администрирования, см. в статье Базы знаний на веб-сайте Службы технической поддержки https://click.kaspersky.com/?hl=en&link=product_compare&pid=KSC&version=11.0.0.
- В хранилище Сервера администрирования вы можете добавить несколько кодов активации и ключей для управляемых программ (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования" на стр. 298).

Особенности лицензирования Kaspersky Security Center

Например, если вы активировали с помощью файла ключа одну из возможностей (например, Управления мобильными устройствами), но вам дополнительно потребовались другие возможности (например, Системного администрирования), в этом случае необходимо приобрести ключ, который активирует обе функциональности, и активировать этим ключом Сервер администрирования.

Особенности лицензирования управляемых программ

Для лицензирования управляемых программ вы можете распространить код активации или ключ автоматически или другим удобным для вас способом. Существуют следующие способы распространения кода активации или ключа:

- Автоматическое распространение.

Если вы используете разные управляемые программы и вам важно распространить определенный ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся ключи на устройства. Например, в хранилище Сервера администрирования находится три ключа. Для всех ключей установлен флажок **Автоматически распространять ключ на управляемые устройства**. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить ключ. Программа определяет, что для этого устройства подходит, например, два ключа из хранилища, ключ *Ключ_1* и ключ *Ключ_2*. На устройство распространяется один из подходящих ключей. В этом случае нельзя предсказать, какой из этих двух ключей будет распространен на данное устройство, так как автоматическое распространение ключей не предполагает вмешательства администратора.

При распространении ключа на устройства происходит подсчет устройств для данного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

- Добавление ключа или кода активации в инсталляционный пакет управляемой программы.

  В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или ключ в инсталляционном пакете или в политике этой программы. Ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

- Распространение с помощью задачи добавления ключа управляемой программы.

  В случае использования задачи добавления ключа управляемой программы вы можете выбрать ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

- Добавление кода активации или ключа вручную на устройства.

Замещение программ безопасности сторонних производителей

Для установки программ безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Kaspersky Security Center предоставляет несколько способов удаления программ сторонних производителей.

Удаление несовместимых программ с помощью программы установки

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых программ поддерживается различными типами установки. Перед установкой программы безопасности несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета программы безопасности (раздел **Несовместимые программы**) установлен флажок **Удалять несовместимые программы автоматически**.

Удаление несовместимых программ при настройке удаленной установки программы

Вы можете включить параметр **Удалять несовместимые программы автоматически** во время настройки удаленной установки программы безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые программы перед установкой программы безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Установка программ с помощью мастера удаленной установки (на стр. 277)

Удаление несовместимых программ с помощью отдельной задачи

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы безопасности не может успешно удалить какую-либо из несовместимых программ.

Инструкции:

- Консоль администрирования: Создание задачи (на стр. 318)

Подготовка к установке программы

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

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

Программы "Лаборатории Касперского". Централизованное развертывание

В этом разделе описаны способы удаленной установки программ "Лаборатории Касперского" и их удаления с устройств сети.

Перед началом установки программ на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует требованиям.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления. На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка программ, и может быть проведена как удаленно, так и локально. При централизованной установке программ безопасности через Консоль администрирования вы можете установить Агент администрирования совместно с программами безопасности.

Агенты администрирования могут отличаться в зависимости от программ "Лаборатории Касперского", с которыми они работают. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в Руководствах к соответствующим программам). Вам нужно установить Агент администрирования на клиентское устройство только один раз.

Управление программами "Лаборатории Касперского" (см. раздел "Список поддерживаемых программ "Лаборатории Касперского" на стр. 30) через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению программой через Kaspersky Security Center плагин управления этой программой должен быть установлен на рабочее место администратора.

Вы можете выполнить удаленную установку программ с рабочего места администратора в главном окне программы Kaspersky Security Center.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

Если удаленная установка программы завершается с ошибкой, вы можете проверить, чем вызвана эта проблема, и устранить ее с помощью утилиты подготовки устройства к удаленной установке (см. раздел "Подготовка устройства к удаленной установке. Утилита riprep.exe" на стр. 289).

Вы можете отслеживать процесс установки программ безопасности "Лаборатории Касперского" в сети с помощью отчета о развертывании.

Подробную информацию об управлении перечисленными программами через Kaspersky Security Center см. в Руководствах к соответствующим программам.

В этом разделе

Установка программ с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в

состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел "Подготовка устройства к удаленной установке. Утилита riprep.exe" на стр. 289).

В этом разделе

Установка программы на выбранные устройства

► *Чтобы установить программу на выбранные устройства, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам устройства.
2. В дереве консоли выберите папку **Задачи**.
3. Запустите процесс создания задачи по ссылке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** выберите тип задачи **Удаленная установка программы**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные устройства.

Установка программы на клиентские устройства группы администрирования

► *Чтобы установить программу на клиентские устройства группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** выберите тип задачи **Удаленная установка программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.
5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на клиентские устройства группы администрирования.

Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы "Лаборатории Касперского" с помощью групповых политик Active Directory.

Установка программ с помощью групповых политик Active Directory возможна только при использовании инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory, выполните следующие действия:*

1. Запустите процесс создания групповой задачи удаленной установки или задачи удаленной установки для набора устройств.
2. В окне мастера удаленной установки **Параметры** установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. В окне мастера удаленной установки **Выбор учетных записей для доступа к устройствам** выберите параметр **Учетная запись требуется (установка без Агента администрирования)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен

Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.

5. В консоли управления групповыми политиками предоставьте следующие разрешения выбранной учетной записи https://support.kaspersky.ru/10639:
   - создание / удаление объектов группы;
   - создание / удаление объектов groupPolicyContainer.
6. Завершите работу мастера.
7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
   - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
   - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).
2. Установка программ на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемой программы.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи установлен флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета

нужной программы.

- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

Установка программ на подчиненные Серверы администрирования.

► *Чтобы установить программу на подчиненные Серверы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета (см. раздел "Распространение инсталляционных пакетов на подчиненные Серверы администрирования" на стр. 286).
3. Запустите создание задачи установки программы на подчиненные Серверы администрирования одним из следующих способов:
   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи удаленной установки для этой группы (см. раздел "Установка программы на клиентские устройства группы администрирования" на стр. 274).
   - Если вы хотите сформировать задачу для определенных подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств (см. раздел "Установка программы на выбранные устройства" на стр. 273).

   В результате запустится мастер создания задачи удаленной установки. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** в папке **Дополнительно** выберите тип задачи **Удаленная установка программы на подчиненные Серверы администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные подчиненные Серверы администрирования.

Установка программ с помощью мастера удаленной установки

Для установки программ компании вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку программ как с использованием сформированных инсталляционных пакетов, так и с дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 и 445; UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. раздел "Подготовка компьютера к удаленной установке.Утилита riprep.exe" " на стр. 289).

► *Чтобы установить программу на выбранные устройства с помощью мастера удаленной установки, выполните следующие действия:*

1. В дереве консоли перейдите к папке **Удаленная установка** и выберите вложенную папку **Инсталляционные пакеты**.
2. В рабочей области папки выберите инсталляционный пакет программы, которую нужно установить.
3. В контекстном меню инсталляционного пакета выберите пункт **Установить программу**.

   Запустится мастер удаленной установки.
4. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлена программа:

   - **Установить на группу управляемых устройств**

     Если выбран этот вариант, задача удаленной установки программы будет создана для группы устройств.

   - **Выбрать устройства для установки**

     Если выбран этот вариант, задача удаленной установки программы будет создана для набора устройств. В состав набора могут входить как устройства в составе групп, так и нераспределенные устройства.
5. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки программы.

   В блоке параметров **Форсировать загрузку инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки программы:

   - **С помощью Агента администрирования**

     Если флажок установлен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

     Если флажок снят, доставка инсталляционных пакетов выполняется средствами

Microsoft Windows.

Рекомендуется установить флажок, если задача назначена для устройств с установленными Агентами администрирования.

По умолчанию флажок установлен.

- **Средствами Microsoft Windows с помощью Сервера администрирования**

  Если флажок установлен, доставка файлов на клиентские устройства будет осуществляться средствами Microsoft Windows с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию флажок установлен.

- **Средствами операционной системы с помощью точек распространения**

  Если флажок установлен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

Если установлен флажок **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию флажок установлен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Количество попыток установки**

Если при запуске задачи удаленной установки Kaspersky Security Center не удается установить программу на управляемое устройство за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку установочного пакета на это управляемое устройство и больше не запускает установку на устройстве.

Параметр `Количество попыток установки` позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует установке. Администратор должен решить проблему в течение указанного количества попыток установки (например, выделив достаточно места на диске, удалив несовместимые программы или изменив параметры других программ, препятствующих установке), и перезапустить задачу (вручную или по расписанию).

Если установка не выполнена, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

Если количество попыток установки, указанное в параметрах задачи, было превышено и устройство готово к установке программы, вы можете увеличить значение параметра Количество попыток установки и запустить задачу по установке программы. Также вы можете создать другую задачу удаленной установки.

Определите, какое действие выполнять с клиентскими устройствами, управляемыми другим Сервером администрирования:

- **Устанавливать всегда**

  Программа устанавливается даже на устройства, управляемые другими Серверами администрирования.

  Параметр выбран по умолчанию; не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

- **Устанавливать на устройства, управляемые только этим Сервером**

  Программа устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними (см. раздел "Избегание конфликтов между Серверами администрирования" на стр. 571).

Настройте дополнительные параметры:

- **Не устанавливать программу, если она уже установлена**

  Если флажок установлен, выбранная программа не устанавливается заново, если она уже установлена на клиентском устройстве.

  Если флажок снят, программа будет установлена в любом случае.

  По умолчанию флажок установлен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если флажок установлен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Флажок доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию флажок снят.

1. В окне **Выбор ключа** выберите лицензионный ключ и способ его распространения:

   - **Не помещать ключ в инсталляционный пакет (рекомендуется)**

     Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

     - если в свойствах ключа настроено автоматическое распространение (см. раздел "Автоматическое распространение лицензионного ключа" на стр. 299);
     - если создана задача **Добавление ключа**.

   - **Поместить ключ в инсталляционный пакет**

Ключ распространяется на устройства вместе с инсталляционным пакетом.

Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу пакетов настроен общий доступ на чтение.

Окно **Выбор ключа** отображается, если в состав инсталляционного пакета не входит лицензионный ключ.

Если в состав инсталляционного пакета входит лицензионный ключ, отображается окно **Свойства ключа** с информацией о лицензионном ключе.

1. В окне **Выбор параметра перезагрузки операционной системы** определите, перезагружать ли устройства, если в ходе установки программ на них потребуется перезагрузка операционной системы:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки программы безопасности.

   - **Перезагрузить устройство**

     Если выбран этот вариант, устройство будет перезагружено после установки программы безопасности.

   - **Спросить у пользователя**

     Если выбран этот вариант, после установки программы безопасности пользователю будет показано сообщение о необходимости перезагрузки устройства. По ссылке **Изменить** можно изменить текст сообщения, а также период отображения сообщения и время выполнения автоматической перезагрузки.

     По умолчанию выбран этот вариант.

   - **Принудительно закрывать программы в заблокированных сеансах**

     Если флажок установлен, программы в заблокированных устройствах будут принудительно закрываться перед перезагрузкой.

     По умолчанию флажок снят.

2. В окне **Выбор учетных записей для доступа к устройствам** можно добавить учетные записи, которые будут использоваться для запуска задачи удаленной установки:

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (установка без Агента администрирования)**

  Если выбран этот вариант, можно указать учетную запись, от имени которой будет запускаться инсталлятор программы. Учетную запись можно указать, в случае если Агент администрирования не установлен на устройствах, для которых назначена задача.

  Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

  Если ни одна учетная запись не добавлена, задача запускается под той учетной записью, под которой работает служба Сервера администрирования.

3. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

   Если в окне **Запуск установки** установлен флажок **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

► *Чтобы установить программу на устройства группы администрирования с помощью мастера удаленной установки, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите пункт **Установить программу**.

   В результате запустится мастер удаленной установки. Следуйте далее указаниям мастера.

4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

После завершения работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии программы. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете запускать эту задачу в дальнейшем вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

► *Чтобы просмотреть отчет о развертывании защиты, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В рабочей области закладки **Отчеты** выберите шаблон отчета **Отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать (см. раздел "Работа с отчетами" на стр. 462):

- для группы администрирования;
- для набора устройств;
- для выборки устройств;
- для всех устройств.

В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлена программа безопасности и включена постоянная защита.

Удаленная деинсталляция программ

Kaspersky Security Center позволяет удаленно деинсталлировать программы с устройств с помощью задач удаленной деинсталляции. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

В этом разделе

Удаленная деинсталляция программы с клиентских устройств группы администрирования

► *Чтобы удаленно деинсталлировать программу с клиентских устройств группы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. Запустите процесс создания задачи по ссылке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.
5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с клиентских устройств группы администрирования.

Удаленная деинсталляция программы с выбранных устройств

► *Чтобы удаленно деинсталлировать программу с выбранных устройств, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам

устройства.

2. В дереве консоли выберите папку **Задачи**.
3. Запустите процесс создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет удалена с выбранных устройств.

Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки программы.

Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

В этом разделе

Создание инсталляционного пакета

► *Чтобы создать инсталляционный пакет, выполните следующие действия:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
   - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Создать** → Инсталляционный пакет;
   - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать** → Инсталляционный пакет;
   - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания инсталляционного пакета. Следуйте далее указаниям мастера.

В процессе создания инсталляционного пакета для программы "Лаборатории Касперского" вам может быть предложено ознакомиться с Лицензионным соглашением на эту программу и Политикой конфиденциальности программы. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения;**
- **Политику конфиденциальности, которая описывает обработку данных.**

Установка программы будет продолжена после установки обоих флажков. После этого создание инсталляционного пакета будет продолжено. Путь к файлу Лицензионного соглашения и Политики конфиденциальности задается в файле с расширением kud или kpd, входящем в состав дистрибутива программы, для которой создается инсталляционный пакет.

> При создании инсталляционного пакета для программы Kaspersky Endpoint Security для Mac вы можете выбрать язык Лицензионного соглашения и Политики конфиденциальности.

Во время создания инсталляционного пакета для программы из базы программ "Лаборатории Касперского" вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), необходимых для установки этой программы. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранной программы. Если инсталляционный пакет создается для патча (неполный дистрибутив), то в список общесистемных компонентов будут включены все необходимые для развертывания патча составляющие, вплоть до версии с полным дистрибутивом. Впоследствии вы можете ознакомиться с этим списком в свойствах инсталляционного пакета.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей

области папки **Инсталляционные пакеты** в дереве консоли.

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке программы Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием следует выбрать файл nagent10.kud, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

При создании инсталляционного пакета Сервера администрирования в качестве файла с описанием следует выбрать файл sc10.kud, расположенный в корневой папке дистрибутива Kaspersky Security Center.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:
   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.
   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center 11** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

   В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.
3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Распространение инсталляционных пакетов с помощью точек распространения

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать точки распространения.

После получения инсталляционных пакетов с Сервера администрирования точки распространения автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с точки распространения.

Передача в Kaspersky Security Center информации о результатах установки программы

После создания инсталляционного пакета программы вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки программы передавалась в Kaspersky Security Center. Для инсталляционных пакетов программ "Лаборатории Касперского" передача диагностической информации о результате установки программы настроена по умолчанию, дополнительная настройка не требуется.

► *Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки программы, выполните следующие действия:*

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранной программы. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.
2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора "Блокнот" Microsoft Windows).

   Файл имеет формат обычного конфигурационного ini-файла.
3. Добавьте в файл следующие строки:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Эта команда настраивает программу Kaspersky Security Center таким образом, чтобы она ожидала окончания установки программы, для которой сформирован инсталляционный пакет и анализировала код возврата программы установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.
4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_SuccessCodes]
   <код возврата>=[<описание>]
   ```

<код возврата 1>=[<описание>]

…

В квадратных скобках приводятся необязательные ключи.

Синтаксис строк:

- <код возврата>. Любое число, соответствующее коду возврата программы установки. Количество кодов возврата может быть произвольным.
- <описание>. Текстовое описание результата установки. Описание может отсутствовать.

5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

   [SetupProcessResult_ErrorCodes]

   <код возврата>=[<описание>]

   <код возврата 1>=[<описание>]

   …

   Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки программы, указанной пользователем, будет записываться в журналах Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

Получение актуальных версий программ

Kaspersky Security Center позволяет получать актуальные версии корпоративных программ, выложенные на интернет-серверах "Лаборатории Касперского".

► *Чтобы получить актуальные версии корпоративных программ "Лаборатории Касперского", выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Security Center.
2. Откройте окно **Актуальные версии программ** по ссылке **Вышли новые версии программ "Лаборатории Касперского"** в блоке **Развертывание**.

   Ссылка **Вышли новые версии программ "Лаборатории Касперского"** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративной программы на интернет-сервере "Лаборатории Касперского".

3. Выберите в списке нужную вам программу.

4. Загрузите дистрибутив программы по ссылке в строке **Веб-адрес дистрибутива**.

Если для выбранной программы отображается кнопка **Загрузить программы и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива программы и автоматического создания инсталляционного пакета. В этом случае Kaspersky Security Center загружает дистрибутив программы на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Список автоматически созданных инсталляционных пакетов отображается в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

После закрытия окна **Актуальные версии программ** ссылка **Вышли новые версии программ "Лаборатории Касперского"** исчезает из блока **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий программ и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Актуальные версии программ** по ссылке **Просмотреть актуальные версии программ "Лаборатории Касперского"** в рабочей области папки **Инсталляционные пакеты**.

См. также:

Установка программ с помощью задачи удаленной установки 272
Установка программ с помощью мастера удаленной установки 277
Просмотр отчета о развертывании защиты 282
Удаленная деинсталляция программ 282
Работа с инсталляционными пакетами 284
Подготовка устройства к удаленной установке. Утилита riprep.exe 289
Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования 293
Создание инсталляционного пакета 285

Подготовка устройства к удаленной установке. Утилита riprep.exe

Удаленная установка программы на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве. В этом случае ее повторное выполнение не требуется.

- Во время запуска задачи устройство было выключено. В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве. Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики устройства (klactgui).
- Если на устройстве не установлен Агент администрирования, при удаленной установке программы могут возникнуть следующие проблемы:
  - на клиентском устройстве включен параметр **Простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для решения проблем, возникших при установке программы на клиентское устройство, на котором не установлен Агент администрирования, вы можете воспользоваться утилитой подготовки устройства к удаленной установке (riprep).

В этом разделе описывается утилита подготовки устройства к удаленной установке (riprep). Она расположена в папке установки Kaspersky Security Center на устройстве с установленным Сервером администрирования.

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

В этом разделе

Подготовка устройства к удаленной установке в интерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в интерактивном режиме, выполните следующие действия:*

1. На клиентском устройстве запустите файл riprep.exe.
2. В открывшемся главном окне утилиты подготовки к удаленной установке установите следующие флажки:
   - **Отключить простой общий доступ к файлам**.
   - **Перезапустить службу Сервера администрирования**.

- **Открыть порты**.
- **Добавить учетную запись**.
- **Отключить контроль учетных записей (UAC)**. Этот параметр доступен для операционных систем Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows Server 2008.

3. Нажмите на кнопку **Запустить**.

В результате в нижней части главного окна утилиты отображаются этапы подготовки устройства к удаленной установке.

Если вы установили флажок **Добавить учетную запись**, при создании учетной записи будет выведен запрос на ввод имени учетной записи и пароля. В результате будет создана локальная учетная запись, принадлежащая группе локальных администраторов.

Если вы установили флажок **Отключить контроль учетных записей**, попытка отключения контроля учетных записей будет выполняться и в том случае, когда до запуска утилиты контроль учетных записей был отключен. После отключения контроля учетных записей будет выведен запрос на перезагрузку устройства.

Подготовка устройства к удаленной установке в неинтерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в неинтерактивном режиме,*

на клиентском устройстве запустите файл riprep.exe из командной строки с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Описания ключей:

- `-silent` – запуск утилиты в неинтерактивном режиме.
- `-cfg CONFIG_FILE` – определение конфигурации утилиты, где `CONFIG_FILE` – путь к файлу конфигурации (файл с расширением .ini).
- `-tl traceLevel` – задание уровня трассировки, где `traceLevel` – число от 0 до 5. Если ключ не задан, то используется значение 0.

В результате запуска утилиты в неинтерактивном режиме вы можете выполнить следующие задачи:

- отключение простого общего доступа к файлам;
- запуск службы Server на клиентском устройстве;
- открытие портов;
- создание локальной учетной записи;
- отключение контроля учетных записей (UAC).

Вы можете задать параметры подготовки устройства к удаленной установке в конфигурационном файле, указанном в ключе `-cfg`. Чтобы задать эти параметры, в конфигурационный файл нужно добавить

следующую информацию:

- В разделе `Common` указать, какие задачи следует выполнять:
  - `DisableSFS` – отключение простого общего доступа к файлам (0 – задача выключена; 1 – задача включена).
  - `StartServer` – запуск службы Server (0 – задача выключена; 1 – задача включена).
  - `OpenFirewallPorts` – открытие необходимых портов (0 – задача выключена; 1 – задача включена).
  - `DisableUAC` – отключение контроля учетных записей (0 – задача выключена; 1 – задача включена).
  - `RebootType` – определение поведения при необходимости перезагрузки при отключенном контроле учетных записей (UAC). Вы можете использовать следующие значения параметра:
    - 0 – никогда не перезагружать устройство;
    - 1 – перезагружать устройство, если до запуска утилиты контроль учетных записей был включен;
    - 2 – перезагружать устройство принудительно, если до запуска утилиты контроль учетных записей был включен;
    - 4 – всегда перезагружать устройство;
    - 5 – всегда принудительно перезагружать устройство.
- В разделе `UserAccount` указать имя учетной записи (`user`) и ее пароль (`Pwd`).

Пример содержимого конфигурационного файла:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

По окончании работы утилиты в папке запуска создаются следующие файлы:

- riprep.txt – отчет о работе, в котором перечислены этапы работы утилиты с причинами их проведения;
- riprep.log – файл трассировки (создается, если заданный уровень трассировки больше 0).

Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования

► *Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования, выполните следующие действия:*

1. Убедитесь, что на целевом устройстве с операционной системой Linux установлена программа sudo.
2. Выполните проверку конфигурации устройства:
   a. Проверьте, что возможно подключение к устройству через SSH (например, программа PuTTY).

      Если вы не можете подключиться к устройству, откройте файл /etc/ssh/sshd_config и убедитесь, что следующие параметры имеют значения:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

      Используйте команду sudo `visudo`, чтобы открыть конфигурационный файл sudoers. В открытом файле укажите: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае username является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.
3. Загрузите и создайте инсталляционный пакет:
   a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (программы, библиотеки) для данного пакета.

      Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

   b. Загрузите инсталляционный пакет Агент администрирования.

   c. Для создания пакета удаленной установки используйте файлы:

      - klnagent.kpd;
      - akinstall.sh;
      - deb или rpm пакет Агента администрирования.
4. Создайте задачу удаленной установки программы с параметрами:

- В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
- В окне **Выбор учетной записи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

5. Запустите задачу удаленной установки программы.

Установка может завершиться ошибкой, если вы устанавливаете Агент администрирования с использованием протокола SSH на устройства с операционными системами Fedora версии ниже 20. В этом случае для успешной установки Агента администрирования в файле /etc/sudoers закомментируйте параметр Defaults requiretty (заключите его в синтаксис комментария, чтобы удалить его из проанализированного кода). Подробное описание того, почему параметр Defaults requiretty может вызвать проблемы при подключении по SSH, вы можете найти на сайте системы отслеживания проблем Bugzilla (https://bugzilla.redhat.com/show_bug.cgi?id=1020147).

Программы "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с ключами управляемых программ "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации программа формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

В этом разделе

Лицензирование управляемых программ

Программы "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения лицензионного ключа или кода активации к каждой из программ. Лицензионный ключ или код активации может быть распространен следующими способами:

- Автоматическое распространение
- с помощью инсталляционного пакета управляемой программы;
- с помощью задачи добавления лицензионного ключа управляемой программы;
- активация управляемой программы вручную.

Автоматическое распространение

Если вы используете разные управляемые программы и вам важно распространить определенный лицензионный ключ или код активации на устройства, используйте другие способы распространения кода активации или лицензионного ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Вы должны включить параметр **Распространять ключ автоматически** для всех трех лицензионных ключей. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Программа определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае нельзя предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение (см. раздел "События превышения лицензионного ограничения" на стр. 266), таким устройствам будет присвоен статус *Критический*.

Перед распространением лицензионный ключ или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 298)
  - Автоматическое распространение лицензионного ключа (см. стр. 299)

Добавление лицензионного ключа или кода активации в инсталляционный пакет управляемой программы

Из соображений безопасности не рекомендуется использовать этот параметр. Лицензионный ключ или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или лицензионный ключ в инсталляционном пакете или в политике этой программы. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
  - Создание инсталляционного пакета (на стр. 285)
  - Установка программ на клиентские устройства (см. стр. 672)

Распространение с помощью задачи добавления лицензионного ключа управляемой программы

В случае использования задачи добавления лицензионного ключа управляемой программы вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением лицензионный ключ или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 298)
  - Распространение лицензионного ключа на клиентские устройства (см. стр. 299)

Добавление кода активации или лицензионного ключа вручную на устройства

Вы можете активировать установленную программу "Лаборатории Касперского" локально, используя инструменты программы. Дополнительную информацию см. в документации к установленным программам.

Просмотр информации об используемых лицензионных ключах

► *Чтобы просмотреть информацию об используемых лицензионных ключах,*

в дереве консоли выберите папку **Лицензии Лаборатории Касперского**.

В рабочей области папки отображается перечень лицензионных ключей, используемых на клиентских устройствах.

Рядом с каждым лицензионным ключом отображается значок, соответствующий типу его использования:

-  – информация об используемом лицензионном ключе получена от подключенного к Серверу администрирования клиентского устройства. Файл этого лицензионного ключа не хранится на Сервере администрирования.
-  – файл ключа находится в хранилище Сервера администрирования. Автоматическое распространение этого лицензионного ключа отключено.
-  – файл ключа находится в хранилище Сервера администрирования. Включено автоматическое

распространение этого лицензионного ключа.

Вы можете просмотреть информацию о том, какие лицензионные ключи используются для активации программы на клиентском устройстве, в разделе **Программы** окна свойств клиентского устройства (см. раздел "Просмотр и изменение локальных параметров программы" на стр. 353).

Для определения актуальных параметров ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки.

Добавление лицензионного ключа в хранилище Сервера администрирования

► *Чтобы добавить лицензионный ключ в хранилище Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Запустите задачу добавления лицензионного ключа одним из следующих способов:
   - в контекстном меню списка лицензионных ключей выберите пункт **Добавить код активации или ключ**;
   - по ссылке **Добавить код активации или ключ** в блоке управления списком лицензионных ключей.

В результате запускается мастер добавления ключа. Следуйте далее указаниям мастера.

Удаление лицензионного ключа Сервера администрирования

► *Чтобы удалить лицензионный ключ Сервера администрирования, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Ключи**.
3. Удалите активный или дополнительный лицензионный ключ по кнопке **Удалить**.

Лицензионный ключ будет удален.

Если добавлен дополнительный лицензионный ключ, после удаления активного лицензионного ключа дополнительный лицензионный ключ автоматически становится активным.

После удаления активного лицензионного ключа для Сервера администрирования (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 257) становятся недоступными функции Системное администрирование и Управление мобильными устройствами (см. раздел "Варианты лицензирования

Kaspersky Security Center" на стр. 257). Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ (см. раздел "Добавление лицензионного ключа в хранилище Сервера администрирования" на стр. 298).

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи распространения лицензионного ключа.

► *Чтобы распространить лицензионный ключ на клиентские устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Нажмите на кнопку **Распространить ключ на управляемые устройства** в блоке управления списком лицензионных ключей.

В результате запустится мастер создания задачи распространения ключа. Следуйте далее указаниям мастера.

Задачи, сформированные при помощи мастера создания задачи распространения ключа, являются задачами для наборов устройств и размещаются в папке **Задачи** дерева консоли.

Вы также можете создать групповую или локальную задачу распространения лицензионного ключа с помощью мастера создания задачи для группы администрирования и для клиентского устройства.

Автоматическое распространение лицензионного ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. В рабочей области папки выберите лицензионный ключ, который вы хотите автоматически распространять на устройства.
3. Откройте окно свойств выбранного лицензионного ключа одним из следующих способов:
   - в контекстном меню лицензионного ключа выберите пункт **Свойства**;
   - по ссылке **Посмотреть свойства ключа** в блоке работы с выбранным лицензионным ключом.
4. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространяемый ключ**. Закройте окно свойств лицензионного ключа.

В результате лицензионный ключ будет автоматически распространяться в качестве активного или дополнительного лицензионного ключа на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Вспомогательные задачи распространения лицензионного ключа для программы при этом не создаются.

При автоматическом распространении лицензионного ключа в качестве активного или дополнительного учитывается лицензионное ограничение на количество устройств. (Лицензионное ограничение задано в свойствах лицензионного ключа.) Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Создание и просмотр отчета об использовании лицензионных ключей

► *Чтобы создать отчет об использовании лицензионных ключей на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите шаблон отчета **Отчет об использовании ключей** или создайте новый шаблон отчета одноименного типа.

В результате в рабочей области отчета об использовании лицензионных ключей отображается информация об активных и дополнительных лицензионных ключах, используемых на клиентских устройствах. Также в отчете содержатся сведения об устройствах, на которых используются лицензионные ключи, и об ограничениях, заданных в свойствах лицензионных ключей.

Процедура приемки

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

В этом разделе

Безопасное состояние

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

Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Сертифицированное состояние программы: параметры и их значения" на стр. 901).

Проверка работоспособности Kaspersky Security Center

После установки Kaspersky Security Center вы можете проверить его работоспособность с помощью выполнения алгоритма проверки. В таблице ниже приведен порядок действий для проверки работоспособности программы и ожидаемые результаты выполнения этих действий.

Таблица 42. Шаги алгоритма проверки работоспособности Kaspersky Security Center

Номер шага	Действие	Результат
1	Подключитесь к Серверу администрирования с помощью Консоли Администрирования (см. раздел "Настройка подключения Консоли администрирования к Серверу администрирования" на стр. 225).	Консоль администрирования подключена к Серверу администрирования. В списке управляемых устройств появилось как минимум одно устройство Сервера администрирования.
2	Выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 213).	Мастер первоначальной настройки создал необходимые для развертывания защиты политики и задачи с параметрами по умолчанию.

Номер шага	Действие	Результат
3	Установите Агент администрирования и Kaspersky Endpoint Security для Windows на устройство (см. раздел "Kaspersky Lab applications. Централизованное развертывание" на стр. 271).	Управляемое устройство, на которое была произведена установка программ, присутствует в списке нераспределенных устройств. В свойствах устройства в разделе **Программы** присутствуют программы Агент администрирования и Kaspersky Endpoint Security для Windows.
4	Загрузите обновления в хранилище Сервера администрирования, запустив задачу загрузки обновлений в хранилище (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. 362). Подробнее см. в Руководстве по эксплуатации, в разделе "Создание задачи загрузки обновлений в хранилище".	Задача завершена успешно и обновления загружены в хранилище.
5	Обновите программу защиты Kaspersky Endpoint Security для Windows. Запустите задачу обновления (см. раздел "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства" на стр. 437). Подробнее см. в Руководстве по эксплуатации, в разделе "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства".	В свойствах управляемого устройства в разделе **Программы** в свойствах программы Kaspersky Endpoint Security для Windows дата последнего обновления баз соответствует дате последнего запуска задачи обновления.

Номер шага	Действие	Результат
6	Внесите произвольные тестовые изменения в политику Kaspersky Endpoint Security для Windows.	Политика применена на управляемом устройстве, обнаруженном в сети: • В свойствах политики присутствует информация о том, что она применена на устройства (см. раздел "Настройка управления запуском программ на клиентских устройствах" на стр. 395). • Параметры программы защиты соответствуют параметрам политики.
7	Скопируйте на одно из управляемых устройств тестовый файл EICAR (см. раздел "Проверка распространения уведомлений" на стр. 234).	В журнале событий есть записи об обнаружении и ликвидации зараженного файла. В свойствах устройства в разделе **Защита** в поле **Обнаружено вирусов** значение увеличилось на один.

Настройка защиты сети

В этом разделе содержится информация о ручной настройке политик, задач и других параметров Сервера администрирования, а также информация о точке распространения, построении структуры групп администрирования, иерархии задач и других настройках.

В этом разделе

Сценарий: Настройка защиты сети

В этом разделе представлен сценарий настройки защиты сети организации. Вы должны использовать сценарий для начальной настройки конфигурации, выполненной в мастере первоначальной настройки.

Оптимизация затрагивает политики и задачи, созданные с параметрами по умолчанию, которые могут оказаться неоптимальными или даже непригодными для данной организации. Поэтому следует просмотреть свойства созданных объектов и, в случае необходимости, внести изменения вручную. Может также потребоваться создать политики и профили политик для программ "Лаборатории Касперского", которые не были созданы мастером первоначальной настройки.

Требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center 11 и завершили основной сценарий развертывания Kaspersky Security Center, включая мастер первоначальной настройки.

Во время работы мастера первоначальной настройки в группе администрирования **Управляемые устройства** создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- политика Агента администрирования;
- Поиск уязвимостей и требуемых обновлений (задача Агента администрирования).

Настройка защиты сети содержит следующие этапы:

a. **Настройка и распространение политик и профилей политик для программ "Лаборатории Касперского"**

   Для настройки и распространения параметров программ "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства (см. раздел "Подходы к управлению безопасностью, ориентированные на устройства и на пользователей" на стр. 309). Можно комбинировать эти два подхода. Для внедрения управления безопасностью, ориентированное на устройства (см. раздел "Настройка и распространение политик:подход, ориентированный на устройства" на стр. 307) метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC).

b. **Настройка задач для удаленного управления программами "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции:

   - Консоль администрирования:
     - Настройка групповой задачи обновления Kaspersky Endpoint Security (см. раздел "Ручная настройка групповой задачи обновления Kaspersky Endpoint Security" на стр. 314)
     - Задание расписания для задачи поиска уязвимостей и требуемых обновлений (задача Агента администрирования) (см. раздел "Настройка расписания задачи Поиск уязвимостей и требуемых обновлений" на стр. 314)

При необходимости создайте дополнительные задачи управления программами "Лаборатории Касперского", установленными на клиентских устройствах (см. раздел "Управление задачами" на стр. 316).

c. **Оценка и ограничение загрузки событий в базу данных**

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

См. также:

- Скорость заполнения событиями базы данных (см. стр. 931)
- Расчет места в базе данных (на стр. 924)

Инструкции:

- Консоль администрирования: Настройка максимального количества событий (см. раздел "Настройка количества событий в хранилище событий" на стр. 315)

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке программ "Лаборатории Касперского", задач и событий, полученных Сервером администрирования.

- Программы "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление программами осуществляется с помощью набора задач.
- Максимальное количество событий, которое может храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и программ "Лаборатории Касперского".

Настройка и распространение политики: подход, ориентированный на устройства

В этом разделе приведен сценарий, ориентированный на устройства, для централизованной настройки программ "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

Требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center.

Процесс

Сценарий управления программами "Лаборатории Касперского", ориентированный на устройства,

содержит следующие шаги:

a. Настройка политик программ

Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждой программы. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для Kaspersky Endpoint Security для Windows. Если вы завершили процесс настройки с помощью этого мастера, у вас нет необходимости создавать новую политику для этой программы. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. стр. 310).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования (см. стр. 329) .

Инструкции:

- Консоль администрирования: Создание политики (на стр. 334)

b. Создание профилей политики (если требуется)

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows, установленные программы "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Консоль администрирования:
  - Создание профиля политики (на стр. 343)

- Создание правила активации профиля политики (см. стр. 345)

c. Распространение политик и профилей политик на управляемые устройства

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно (см. раздел "Принудительная синхронизация" на стр. 598). После завершения синхронизации политики и профили политик доставляются и применяются к установленным программам "Лаборатории Касперского".

Инструкции:

- Консоль администрирования: Принудительная синхронизация (на стр. 598)

Результаты

После завершения сценария, ориентированного на устройства, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики программ и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

См. также:

Основной сценарий развертывания и другие сценарии развертывания 49
Иерархия Серверов администрирования 34
Группы администрирования 38
Политики 40
О профилях политики 41
Иерархия политик 329

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователя*. Чтобы применить разные параметры программ к разным устройствам, вы можете использовать один или оба типа управления в комбинации. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC). Для реализации ориентированного на пользователей метода управления

безопасностью подходит только Kaspersky Security Center 11 Web Console.

Управление безопасностью, ориентированное на устройства (см. раздел "Настройка и распространение политик:Управление безопасностью, ориентированное на устройства на стр. 307) основано на применении различных параметров безопасности к управляемым устройствам. Выбор параметров зависит от специфических для устройства функций, таких как расположение устройств в группах администрирования, использование этих устройств в Active Directory, или от спецификации программного обеспечения устройств.

Управление безопасностью, ориентированной на пользователя основано на применении различных параметров безопасности для управления устройствами. Выбор параметров зависит от ролей пользователей, которым принадлежат эти устройства. Например, можно применить различные параметры программ к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдела кадров – получит свои собственные права для работы с программами "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры программы могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры программ для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать инциденты безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры программы. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики (см. раздел "Политики" на стр. 40) для каждой группы администрирования, а затем дополнительно создать профили политик (см. раздел "О профилях политики" на стр. 41) для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки Kaspersky Security Center. Настройка выполняется в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

В этом разделе

Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

Ниже описаны действия по дополнительной настройке, которую рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Продвинутая защита**.

Раздел Продвинутая защита, подраздел Kaspersky Security Network

Рекомендуется включить параметр **Использовать прокси-сервер KSN**. Это значительно увеличит надежность обнаружения вредоносных программ.

Можно также включить использование серверов KSN, если служба прокси-сервера KSN недоступна. Серверы KSN могут располагаться как на стороне "Лаборатории Касперского" (при использовании Глобального KSN), так и у третьих сторон (при использовании Локального KSN).

Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

Ниже описаны действия по дополнительной настройке, которую рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Базовая защита**.

Раздел Базовая защита, подраздел Сетевой экран

Следует проверить список сетей в свойствах политики. В списке могут отображаться не все сети.

► *Чтобы проверить список сетей, выполните следующие действия:*

1. В свойствах политики в разделе **Базовая защита** выберите подраздел **Сетевой экран**.

2. В блоке **Доступные сети** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**. Список сетей отображается в этом окне на закладке **Сети**.

Раздел Базовая защита, подраздел Защита от файловых угроз

Включенная проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

► *Чтобы выключить проверку сетевых дисков, выполните следующие действия:*

1. В свойствах политики в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Защита от файловых угроз** на закладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

Ниже описаны действия по дополнительной настройке, которые рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Общие параметры**.

Раздел Дополнительные параметры, подраздел Отчеты и хранилища

В блоке **Информировать Сервер администрирования** следует обратить внимание на следующий параметр:

Флажок **О запускаемых программах** – если флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов). Поэтому в политике верхнего уровня флажок **О запускаемых программах** следует снять, если он оказался установлен.

Раздел Дополнительные параметры, подраздел Интерфейс

Если защита в сети организации должна управляться полностью централизованно через Консоль администрирования, то следует выключить отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях (снять флажок **Отображать интерфейс программы** в разделе **Взаимодействие с пользователем**), а также включить защиту паролем (установить флажок **Включить защиту паролем** в разделе **Защита паролем**).

Настройка политики в разделе Настройка событий

В разделе **Настройка событий** следует отключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На закладке **Критическое событие**:
  - Автозапуск программы выключен.
  - Доступ запрещен.
  - Запуск программы запрещен.
  - Лечение невозможно.
  - Нарушено Лицензионное соглашение.
  - Не удалось загрузить модуль шифрования.
  - Невозможен запуск двух задач одновременно.
  - Обнаружена активная угроза. Требуется запуск процедуры лечения.
  - Обнаружена сетевая атака.
  - Обновлены не все компоненты.
  - Ошибка активации.
  - Ошибка активации портативного режима.
  - Ошибка взаимодействия с Kaspersky Security Center.
  - Ошибка деактивации портативного режима.
  - Ошибка изменения состава программы.
  - Ошибка применения правил шифрования / расшифровки файлов.
  - Политика не может быть применена.
  - Процесс завершен.
  - Сетевая активность запрещена.
- На закладке **Отказ функционирования**:
  - Ошибка в параметрах задачи. Параметры задачи не применены.
- На закладке **Предупреждение**:
  - Самозащита программы выключена.
  - Некорректный резервный код активации.
  - Пользователь отказался от политики шифрования.
- На закладке **Информационное сообщение**:
  - Запуск программы запрещен в тестовом режиме.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Информация в этом подразделе применима для Kaspersky Security Center 10 Maintenance Release 1 и более поздних версий.

Оптимальным и рекомендуемым расписанием для Kaspersky Endpoint Security версии 10 и выше является **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Для групповой задачи обновления Kaspersky Endpoint Security версии 8 следует явно указать период запуска (1 час или больше) и установить флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений

Мастер первоначальной настройки создает для Агента администрирования групповую задачу поиска уязвимостей и требуемых обновлений. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача поиска уязвимостей и требуемых обновлений будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, флажок **Запускать пропущенные задачи** снят.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программа вычисляет приблизительный размер дискового пространства для хранения указанного количества событий. Когда вы указываете максимальное количество событий, программы вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые. Несмотря на то, что Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

► *Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **ОК**.

Количество событий, хранящихся в базе данных, будет ограничено указанным значением.

Управление задачами

Kaspersky Security Center управляет работой программ, установленных на устройствах, путем создания и запуска различных задач. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Задачи делятся на следующие типы:

- *Групповые задачи*. Задачи, которые выполняются на устройствах выбранной группы администрирования.
- Задачи Сервера администрирования. Задачи, которые выполняются на Сервере администрирования.
- *Задачи для наборов устройств*. Глобальные задачи – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.
- *Локальные задачи*. Локальные задачи – это задачи, которые выполняются на конкретном устройстве.

Создание задач для программы возможно только в случае, если на рабочее место администратора установлен плагин управления этой программой.

Список устройств, для которых будет создана задача, можно сформировать одним из следующих способов:

- Выбрать устройства, обнаруженные в сети Сервером администрирования.
- Задать список устройств вручную. В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.
- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования при подключении устройств или в результате обнаружения устройств.

Для каждой программы вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Обмен информацией о задачах между программой, установленной на устройстве, и информационной базой Kaspersky Security Center происходит в момент соединения Агента администрирования с Сервером администрирования.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи. При остановке программы выполнение всех запущенных задач прекращается.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и в Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

Управление задачами для программ, поддерживающих мультиарендность

Групповая задача для мультиарендных программ применяется к программам в зависимости от иерархии Серверов администрирования и клиентских устройств. Виртуальный Сервер администрирования, на котором создана задача, должен быть в той же группе администрирования, что и клиентское устройство, на котором установлена программа, или в группе более низкого уровня.

В событиях, которые соответствуют результатам выполнения задачи, администратору поставщика услуг отображается информация об устройстве, на котором выполнена задача. В свою очередь, администратору отображается **Мультиарендный узел**.

В этом разделе

Создание групповой задачи

В Консоли администрирования можно создавать задачи непосредственно в папке группы администрирования, для которой создается задача, и в рабочей области папки **Задачи**.

► *Чтобы создать задачу в папке группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать задачу.
2. В рабочей области выберите закладку **Задачи**.
3. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

► *Чтобы создать задачу в рабочей области папки **Задачи**, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

Создание задачи Сервера администрирования

Сервер администрирования выполняет следующие функции:

- автоматическое распространение обновлений;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На виртуальном Сервере администрирования доступна только задача автоматической рассылки отчетов и задача создания инсталляционного пакета на основе образа операционной системы эталонного устройства. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования. Резервное копирование данных виртуального Сервера осуществляется в рамках резервного копирования данных главного Сервера администрирования.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать → Задачу**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Задачи Загрузка обновлений в хранилище Сервера администрирования, Синхронизация обновлений Windows Update, Обслуживание базы данных и Резервное копирование данных Сервера администрирования можно создать только в одном экземпляре. Если задачи Загрузка обновлений в хранилище Сервера администрирования, Обслуживание базы данных, Резервное копирование данных Сервера администрирования и Синхронизация обновлений Windows Update уже созданы для Сервера администрирования, то они не отображаются в окне выбора типа задачи мастера создания задачи.

Создание задачи для набора устройств

В Kaspersky Security Center можно создавать задачи для произвольно выбранного набора устройств. Устройства в наборе могут входить в разные группы администрирования или не входить ни в одну группу администрирования. Kaspersky Security Center позволяет выполнять следующие основные задачи для набора устройств:

- Удаленная установка программ.
- сообщение для пользователя (см. раздел "Отправка сообщения пользователям устройств" на стр. 599);
- смену Сервера администрирования (см. раздел "Смена Сервера администрирования для клиентских устройств" на стр. 596);
- управление устройством (см. раздел "Удаленное включение, выключение и перезагрузка клиентских устройств" на стр. 597);
- проверку обновлений (см. раздел "Проверка полученных обновлений" на стр. 373);
- распространение инсталляционных пакетов (см. раздел "Распространение инсталляционных пакетов на подчиненные Серверы администрирования" на стр. 286);
- установка программ на подчиненные Серверы администрирования (см. раздел "Установка программ на подчиненные Серверы администрирования" на стр. 276).
- Удаленная деинсталляция программы (см. раздел "Удаленная деинсталляция программ" на стр. 282).

► *Чтобы создать задачу для набора устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Создание локальной задачи

► *Чтобы создать задачу рассылки нескольких отчетов, выполните следующие действия:*

1. В рабочей области группы, в состав которой входит устройство, выберите закладку **Устройства**.
2. В списке устройств на закладке **Устройства** выберите устройство, для которого нужно создать локальную задачу.
3. Запустите процесс создания задачи для выбранного устройства одним из следующих способов:
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Создать задачу**.
   - В рабочей области папки Задачи нажмите на кнопку **Создать задачу**.
   - Из окна свойств устройства следующим образом:
     a. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
     b. В открывшемся окне свойств устройства выберите раздел **Задачи** и нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Подробные описания создания и настройки локальных задач приводятся в Руководствах к соответствующим программам "Лаборатории Касперского".

Отображение унаследованной групповой задачи в рабочей области вложенной группы

► *Чтобы включить отображение унаследованных задач вложенной группы в рабочей области, выполните следующие действия:*

1. Выберите в рабочей области вложенной группы закладку **Задачи**.
2. В рабочей области закладки **Задачи** нажмите на кнопку **Показывать унаследованные задачи**.

В результате унаследованные политики отображаются в списке политик со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования редактирование унаследованных задач доступно только в той группе, в которой они были созданы. Редактирование унаследованных задач недоступно в той группе, которая наследует задачи.

Автоматическое включение устройств перед запуском задачи

Kaspersky Security Center позволяет настроить параметры задачи так, чтобы перед выполнением задачи на выключенных устройствах загружалась операционная система.

► *Чтобы настроить автоматическое включение устройств перед запуском задачи, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Активировать устройство перед запуском задачи функцией Wake On Lan за (мин)** и укажите время в минутах.

В результате выключенные устройства будут автоматически включены за указанное количество минут до запуска задачи, и на них будет загружена операционная система.

Автоматическая загрузка операционной системы доступна только на устройствах с поддержкой функции Wake On LAN.

Автоматическое выключение устройства после выполнения задачи

Kaspersky Security Center позволяет настроить параметры задачи таким образом, чтобы после ее выполнения устройства, на которые она распространяется, автоматически выключались.

► *Чтобы устройства автоматически выключались после выполнения задачи, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Выключать устройство после выполнения задачи**.

Ограничение времени выполнения задачи

► *Чтобы ограничить время выполнения задачи на устройствах, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с клиентскими устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Остановить, если задача выполняется дольше (мин)** и укажите время в минутах.

В результате, если по истечении указанного времени выполнение задачи на устройстве не будет

завершено, Kaspersky Security Center автоматически остановит выполнение задачи.

Экспорт задачи

Вы можете экспортировать групповые задачи и задачи для наборов устройств в файл. Задачи Сервера администрирования и локальные задачи недоступны для экспорта.

► *Чтобы экспортировать задачу, выполните следующие действия:*

1. В контекстном меню задачи выберите пункт **Все задачи** → **Экспорт**.
2. В открывшемся окне **Сохранить как** укажите имя файла и путь для сохранения.
3. Нажмите на кнопку **Сохранить**.

Права локальных пользователей не экспортируются.

Импорт задачи

Вы можете импортировать групповые задачи и задачи для наборов устройств. Задачи Сервера администрирования и локальные задачи недоступны для импорта.

► *Чтобы импортировать задачу, выполните следующие действия:*

1. Выберите список задач, в который требуется импортировать задачу:
   - Если вы хотите импортировать задачу в список групповых задач, в рабочей области нужной вам группы администрирования выберите закладку **Задачи**.
   - Если вы хотите импортировать задачу в список задач для наборов устройств, в дереве консоли выберите папку **Задачи**.
2. Выберите один из следующих способов импорта задачи:
   - В контекстном меню списка задач выберите пункт **Все задачи** → **Импортировать**.
   - По ссылке **Импортировать задачу из файла** в блоке управления списком задач.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу.
4. Нажмите на кнопку **Открыть**.

В результате импортированная задача отобразится в списке задач.

Если в выбранном списке уже существует задача с именем, аналогичным имени импортируемой задачи, к имени импортируемой задачи будет добавлено окончание вида **(<порядковый номер>)** например: **(1)**, **(2)**.

Конвертация задач

С помощью Kaspersky Security Center можно конвертировать задачи предыдущих версий программ "Лаборатории Касперского" в задачи текущих версий программ.

Конвертация возможна для задач следующих программ:

- Антивирус Касперского 6.0 для Windows Workstations MP4;
- Kaspersky Endpoint Security 8 для Windows.
- Kaspersky Endpoint Security 10 для Windows.

► *Чтобы конвертировать задачи, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию задач.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи → Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

В результате работы мастера формируются новые задачи, использующие параметры задач предыдущих версий программ.

Запуск и остановка задачи вручную

Задачи можно запускать и останавливать двумя способами: из контекстного меню задачи и в окне свойств клиентского устройства, которому назначена эта задача.

Запускать групповые задачи из контекстного меню устройства могут пользователи, входящие в группу **KLAdmins** (см. раздел "Права доступа к Серверу администрирования и его объектам" на стр. 548).

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств задачи, выполните следующие действия:*

1. В списке задач выберите задачу.

2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Запустить** или **Остановить** .
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Запустить** или **Остановить**.

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств клиентского устройства, выполните следующие действия:*

1. В списке устройств выберите устройство.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню устройства выберите пункт **Все задачи** → **Запустить задачу**. Из списка задач выберите требуемую.

     Список устройств, для которых назначена задача, будет замещен выбранным устройством. Задача будет запущена.
   - В окне свойств устройства в разделе **Задачи** нажмите на кнопку  или  .

Приостановка и возобновление задачи вручную

► *Чтобы приостановить или возобновить выполнение запущенной задачи, выполните следующие действия:*

1. В списке задач выберите задачу.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Приостановить** или **Возобновить**.
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Приостановить** или **Возобновить**.

Наблюдение за ходом выполнения задачи

► *Чтобы наблюдать за ходом выполнения задачи,*

в окне свойств задачи выберите раздел **Общие**.

В средней части окна раздела **Общие** содержится информация о текущем состоянии задачи.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Просмотр результатов выполнения локальных задач недоступен.

► *Чтобы посмотреть результаты выполнения задачи, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Настройка фильтра информации о результатах выполнения задачи

Kaspersky Security Center позволяет фильтровать информацию о результатах выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Для локальных задач фильтрация недоступна.

► *Чтобы настроить фильтр для информации о результатах выполнения задачи, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

   Таблица в верхней части окна содержит список всех устройств, для которых назначена задача. Таблица в нижней части окна содержит результаты выполнения задачи на выбранном устройстве.
3. В интересующей вас таблице по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Фильтр**.
4. В открывшемся окне **Применить фильтр** настройте параметры фильтра в разделах окна **События**, **Устройства** и **Время**. Нажмите на кнопку **ОК**.

В результате в окне **Результаты выполнения задачи** будет отображаться информация, удовлетворяющая параметрам, заданным в фильтре.

Изменение задачи. Откат изменений

► *Чтобы изменить задачу, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу и с помощью контекстного меню перейдите в окно свойств задачи.
3. Внесите необходимые изменения.

   В разделе **Исключения из области действия задачи** можно настроить список вложенных групп, на которые не будет распространяться задача.
4. Нажмите на кнопку **Применить**.

Изменения задачи будут сохранены в окне свойств задачи, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения задачи.

► *Чтобы откатить изменения задачи, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Выберите задачу, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств задачи.
3. В окне свойств задачи выберите раздел **История ревизий**.
4. В списке ревизий задачи выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение задач

Вы можете сравнивать задачи одного типа, например, можно сравнить две задачи антивирусной проверки, но нельзя сравнить задачу антивирусной проверки с задачей установки обновлений. В результате сравнения задач вы получаете отчет, показывающий, какие параметры задач совпадают, а какие различаются. Вы можете распечатать отчет сравнения задач или сохранить его в файле. Сравнение задач может потребоваться в случае, когда для разных подразделений одной компании есть различные задачи одного типа. Например, для бухгалтерии есть задача проверять на вирусы только локальные диски компьютера, а для отдела продаж, сотрудники которого переписываются с клиентами, есть задача проверять и локальные диски, и почту. Чтобы быстро увидеть такие различия, нет необходимости просматривать все параметры задачи, достаточно выполнить сравнение задач.

Сравнение можно выполнить только для задач одного типа.
Задачи можно сравнивать только попарно.

Вы можете сравнивать задачи одним из следующих способов: путем выбора одной задачи и сравнения ее с другой или путем сравнения любых двух задач из списка задач.

► *Чтобы выбрать одну задачу и сравнить ее с другой, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу, которую нужно сравнить с другой задачей.
3. В контекстном меню задачи выберите пункт **Все задачи** → **Сравнить с другой задачей**.
4. В окне **Выбор задачи** выберите задачу для сравнения.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух задач в формате HTML.

► *Чтобы сравнить две задачи из списка задач, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** в списке задач с помощью клавиши **SHIFT** или **CTRL** выберите две задачи одного типа.
3. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения выбранных задач в формате HTML.

При сравнении задач, в случае если используемые пароли отличаются, в отчете сравнения задач будут отображаться символы ******.

Если в свойствах задачи был изменен пароль, в отчете сравнения ревизий задачи будут отображаться символы ******.

Учетные записи для запуска задач

Вы можете задавать учетную запись, под которой должна запускаться задача.

Например, для выполнения задач проверки по требованию необходимы права на доступ к проверяемому объекту, а для выполнения задач обновления – права авторизованного пользователя прокси-сервера. Возможность задать учетную запись для запуска задачи позволяет избежать ошибки при выполнении задач проверки по требованию и задач обновления, если у пользователя, запустившего задачу, нет необходимых прав доступа.

В задачах удаленной установки и деинсталляции программы учетная запись используется для загрузки на клиентские устройства файлов, необходимых для установки (удаления), если на устройстве не установлен или недоступен Агент администрирования. При установленном и доступном Агенте администрирования учетная запись используется, если согласно параметрам задачи доставка файлов выполняется только средствами Microsoft Windows из папки общего доступа. В этом случае учетная запись должна обладать следующими правами на устройстве:

- правом на удаленный запуск программ;
- правами на ресурс Admin$;
- правом *Вход в качестве службы*.

Если доставку файлов на устройства выполняет Агент администрирования, учетная запись использоваться не будет. Все операции по копированию и установке файлов будет выполнять **Агент администрирования** (**Учетная запись LocalSystem**).

Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу

администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования (см. раздел "Группы администрирования" на стр. 38).

В состав групп администрирования, подчиненных виртуальному Серверу администрирования, нельзя добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования (см. стр. 89).

См. также:

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В разделе также содержится информация о профилях политик, которые поддерживаются в Kaspersky Security Center, начиная с версии 10 Service Pack 1.

В этом разделе

Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики программы P, определенной для группы G, являются управляемые устройства с установленной программой P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием замков () возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одной и той же программы действуют друг на друга по иерархии групп администрирования: параметры с установленным замком из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Политика для автономных пользователей не будет поддерживаться в будущих версиях Kaspersky Security Center. Вместо политик для автономных пользователей следует использовать профили политик.

Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Во избежание подобных проблем в Kaspersky Security Center, начиная с версии 10 Service Pack 1, поддерживаются *профили политики*. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров политики распространяется на устройства вместе с политикой и дополняет политику при выполнении некоторого условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в

профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).

- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования (см. раздел "Настройка профилей соединения для автономных пользователей" на стр. 226);
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Неоднозначность устраняется при помощи приоритетов профилей: значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Наследование параметров политики

Политика задается для группы администрирования. Параметры политики могут *наследоваться*, то есть передаваться в подгруппы (дочерние группы) групп администрирования, для которых она создана. Политика, созданная для родительской группы, также называется *родительской политикой*.

Можно включить или выключить два параметра наследования: **Наследовать параметры родительской политики** и **Форсировать наследование параметров дочерними политиками**.

- Если вы включили **Наследовать параметры родительской политики** для дочерней политики и заблокировали некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры для дочерней группы. Однако вы можете изменить параметры, которые не заблокированы в родительской политике.
- Если вы выключили **Наследовать параметры родительской политики** для дочерней политики, тогда вы можете изменить все параметры в дочерней группе, даже если некоторые параметры заблокированы в родительской политике.
- Если в родительской группе включен параметр **Форсировать наследование параметров дочерними политиками**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.
- В политиках для группы **Управляемые устройства** параметр **Наследовать параметры родительской политики** не влияет ни на какие параметры, так как группа **Управляемые устройства** не имеет вышестоящих групп и, следовательно, не наследует никакие политики.

По умолчанию параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

Управление политиками

Централизованная настройка параметров программ, установленных на клиентских устройствах, осуществляется через определение политик.

Политики, сформированные для программ в группе администрирования, отображаются в рабочей области на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (см. раздел "Статусы устройств, задач и политик" на стр. 862).

После удаления политики или прекращения ее действия программа продолжает работу с параметрами,

заданными в политике. В дальнейшем эти параметры можно изменить вручную.

Применение политики производится следующим образом: если на устройстве выполняются резидентные задачи (задачи постоянной защиты), их выполнение продолжается с новыми значениями параметров. Запущенные периодические задачи (проверка по требованию, обновление баз программ) выполняются с неизмененными значениями. Новый запуск периодических задач производится с измененными значениями параметров.

Политики для программ с поддержкой мультиарендности наследуются для групп администрирования более низкого уровня, а также для групп администрирования верхнего уровня: политика распространяется на все клиентские устройства, на которых установлена программа.

В случае использования иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские устройства. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого изменения, внесенные в параметры политики, распространяются на унаследованные политики на подчиненных Серверах администрирования.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространятся на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским устройством, на устройстве вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Результаты распространения политики на клиентские устройства отображаются в окне свойств политики Сервера администрирования, к которому они подключены.

Не используйте в параметрах политик конфиденциальные данные. Например, пароль доменного администратора.

В этом разделе

Создание политики

В Консоли администрирования можно создавать политики непосредственно в папке группы администрирования, для которой создается политика, и в рабочей области папки **Политики**.

► *Чтобы создать политику в папке группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите закладку **Политики**.
3. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

► *Чтобы создать политику в рабочей области папки **Политики**, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых программа не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Вы можете изменять политику после ее создания.

Не используйте в параметрах политик конфиденциальные данные. Например, пароль доменного администратора.

Параметры программ "Лаборатории Касперского", которые изменяются после применения политик, подробно описаны в Руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен "замок" ), начинают действовать на клиентских устройствах независимо от того, какие параметры были определены для программы ранее.

Отображение унаследованной политики во вложенной группе

► *Чтобы включить отображение унаследованных политик для вложенной группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно отображать унаследованные политики.
2. В рабочей области группы выберите закладку **Политики**.
3. В контекстном меню списка политик выберите пункт **Вид** → **Унаследованные политики**.

В результате унаследованные политики отображаются в списке политик со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования параметров изменение унаследованных политик доступно только в той группе, в которой они были созданы. Изменение унаследованных политик недоступно в

той группе, которая наследует политики.

Активация политики

► *Чтобы сделать политику активной для выбранной группы, выполните следующие действия:*

1. В рабочей области группы на закладке **Политики** выберите политику, которую нужно сделать активной.
2. Для активации политики выполните одно из следующих действий:
   - В контекстном меню политики выберите пункт **Активная политика**.
   - В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских устройств на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака", выполните следующие действия:*

1. В окне свойств Сервера администрирования откройте раздел **Вирусная атака**.
2. Откройте окно **Активация политик** по ссылке **Настроить активацию политик по возникновению события "Вирусная атака"** и добавьте политику в выбранный список политик, активируемых при обнаружении вирусной атаки.

В случае активации политики по событию *Вирусная атака* вернуться к предыдущей политике можно только вручную.

Применение политики для автономных пользователей

Политика для автономных пользователей вступает в силу на устройстве в случае его отключения от сети организации.

► *Чтобы применить выбранную политику для автономных пользователей,*

в окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите

вариант **Политика для автономных пользователей**.

В результате политика начинает действовать на устройствах в случае их отключения от сети организации.

Изменение политики Откат изменений

► *Чтобы изменить политику, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Применить**.

Изменения политики будут сохранены в свойствах политики, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения политики.

► *Чтобы откатить изменения политики, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. Выберите политику, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств политики.
3. В окне свойств политики выберите раздел **История ревизий**.
4. В списке ревизий политики выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение политик

Вы можете сравнивать две политики для одной управляемой программы. В результате сравнения политик вы получаете отчет, показывающий, какие параметры политик совпадают, а какие различаются. Сравнивать политики бывает нужно, например, если разные администраторы в своих локальных офисах создали несколько политик для одной управляемой программы или если одна политика верхнего уровня была унаследована и изменена для каждого локального офиса. Вы можете сравнивать политики одним из следующих способов: путем выбора одной политики и сравнения ее с другой или путем сравнения любых двух политик из списка политик.

► *Чтобы сравнить политику с другой политикой, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику, которую нужно сравнить с другой политикой.

3. В контекстном меню политики выберите пункт **Сравнить политику с другой политикой**.
4. В окне **Выбор политики** выберите политику, с которой нужно провести сравнение.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

► *Чтобы сравнить две политики из списка политик, выполните следующие действия:*

1. В папке **Политики** в списке политик с помощью клавиши **SHIFT** или **CTRL** выберите две политики для одной управляемой программы.
2. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

В отчете сравнения параметров политик для программы Kaspersky Endpoint Security для Windows выполняется также сравнение профилей политики. Результаты сравнения параметров профилей политик можно свернуть. Чтобы свернуть блок, нажмите на треугольный значок рядом с названием блока.

Удаление политики

► *Чтобы удалить политику, выполните следующие действия:*

1. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую нужно удалить.
2. Удалите политику одним из следующих способов:
   - В контекстном меню политики выберите пункт **Удалить**.
   - Перейдите по ссылке **Удалить политику** в информационном окне выбранной политики.

Копирование политики

► *Чтобы скопировать политику, выполните следующие действия:*

1. В рабочей области нужной вам группы на закладке **Политики** выберите политику.
2. В контекстном меню политики выберите пункт **Копировать**.
3. Выберите в дереве консоли группу, в которую требуется добавить политику.

   Политику можно добавить в ту же группу, из которой она скопирована.
4. В контекстном меню списка политик для выбранной группы на закладке **Политики** выберите пункт **Вставить**.

В результате политика копируется с сохранением всех параметров и распространяется на устройства группы, в которую она перенесена. Если вы вставляете политику в ту же группу, из которой она была скопирована, к имени политики автоматически добавляется окончание вида **(<порядковый номер>)**,

например: **(1)**, **(2)**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной.

Экспорт политики

► *Чтобы экспортировать политику, выполните следующие действия:*

1. Удалите политику одним из следующих способов:
   - В контекстном меню политики выберите пункт **Все задачи** → **Экспорт**.
   - Перейдите по ссылке **Экспорт политики в файл** в информационном окне для выбранной политики.
2. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

Импорт политики

► *Импорт политики*

1. В рабочей области нужной вам группы на закладке **Политики** выберите один из следующих способов импорта политики:
   - В контекстном меню списка политик выберите пункт **Все задачи** → **Импорт**.
   - По ссылке **Импортировать политику из файла** в блоке управления списком политик.
2. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

В результате добавленная политика отображается в списке политик.

Если в выбранном списке политик уже существует политика с именем, аналогичным имени импортируемой политики, к имени импортируемой политики будет добавлено окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Конвертация политик

Kaspersky Security Center может конвертировать политики предыдущих версий программ "Лаборатории Касперского" в политики текущих версий этих программ.

Конвертация возможна для политик следующих программ:

- Антивирус Касперского 6.0 для Windows Workstations MP4;
- Kaspersky Endpoint Security 8 для Windows.
- Kaspersky Endpoint Security 10 для Windows.

► *Чтобы конвертировать политики, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию политик.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

В результате работы мастера формируются новые политики, использующие параметры политик предыдущих версий программ "Лаборатории Касперского".

Управление профилями политик

Этот раздел содержит информацию о профилях политик, которые используются для эффективного управления группами клиентских устройств. Описаны преимущества профилей политик, способы их применения. В разделе также приведены инструкции по созданию, настройке и удалению профилей политик.

В этом разделе

О профиле политики

Профиль политики – это именованный набор параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве), если устройство удовлетворяет заданным правилам активации (см. раздел "Создание правила активации профиля политики" на стр. 345). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли

иметь разные параметры политики. Например, возможна ситуация, когда в группе администрирования для некоторых устройств параметры политики должны быть изменены. В этом случае для такой политики можно настроить профили политики, использование которых позволяет изменять параметры политики не для всех устройств группы администрирования. Например, политика запрещает запуск программ городской навигации для всех устройств группы администрирования "Пользователи". Программы городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". На этом устройстве можно установить тег "Курьер" и настроить профиль политики таким образом, чтобы был разрешен запуск программ городской навигации только на устройстве с тегом "Курьер", с сохранением всех остальных параметров политики. В этом случае если в группе администрирования "Пользователи" появляется устройство с тегом "Курьер", на нем будет разрешен запуск программ городской навигации. Запуск программ городской навигации на других устройствах в группе администрирования "Пользователи", у которых тег "Курьер" отсутствует, будет запрещен.

Профили поддерживаются только для следующих политик:

- политики программы Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше;
- политики программы Kaspersky Endpoint Security 10 Service Pack 1 для Mac;
- политики плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1;
- политики плагина Kaspersky Device Management для iOS.

Преимущества профилей политик

Профили политик облегчают управление клиентскими устройствами, на которых применены политики:

- Параметры профиля политики могут отличаться от параметров самой политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Вы можете экспортировать и импортировать профили политики, а также создавать новые профили на основе существующих.
- Для одной политики несколько профилей политики могут быть активными. К устройству будут применены те из профилей, которые удовлетворяют правилам активации на этом устройстве.
- Профили подчиняются иерархии политик. Унаследованная политика содержит все профили политики верхнего уровня.

Приоритеты профилей

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится выше профиля Y в списке профилей, то профиль X имеет более высокий приоритет, чем Y. К одному устройству одновременно могут быть применены несколько профилей. Если значение какого-то параметра различается в профилях, на устройстве применится значение параметра из того профиля, который имеет более высокий приоритет.

Правила активации профиля

Профиль политики активируется на клиентском устройстве при выполнении правила активации. *Правила активации* – набор условий, при выполнении которых профиль политики начинает работать на устройстве. Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство явно (устройство находится непосредственно в указанном подразделении) или неявно (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности) размещено в определенном подразделении Active Directory®, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center.
- Владельцу устройства была назначена определенная роль.

Политики в иерархии групп администрирования

Если вы создаете политику в группе администрирования нижнего уровня, то новая политика наследует профили активной политики для группы верхнего уровня. Профили с одинаковыми именами объединяются. Профили политики для группы более высокого уровня имеют более высокий приоритет. Например, в группе администрирования *A* политика *P(A)* имеет профили *X1*, *X2*, и *X3*, в порядке убывания приоритета. В группе администрирования *B*, которая является подгруппой группы *A*, создана политика *P(B)*, с профилями *X2*, *X4*, *X5*. Тогда политика *P(B)* будет изменена политикой *P(A)*, так, что в политике *P(B)* список профилей в порядке убывания приоритета будет *X1*, *X2*, *X3*, *X4*, *X5*. Приоритет профиля *X2* будет зависеть от начального состояния *X2* политики *P(B)* и *X2* политики *P(A)*. После создания политики *P(B)* политика *P(A)* не будет отображаться в подгруппе *B*.

Активная политика вычисляется каждый раз заново при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству. Например, устройству увеличили объем оперативной памяти, в результате активировался профиль политики, который применяется для устройств с большим объемом оперативной памяти.

Свойства и ограничения профиля политики

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если политика активна в автономном режиме, то и профили этой политики применяются только в автономном режиме.
- Профили не поддерживают статический анализ доступа к исполняемым файлам (см. раздел "Просмотр результатов статического анализа правил запуска исполняемых файлов" на стр. 396).

- Профиль политики не может содержать параметры оповещений о событиях.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики активируется в течение одной минуты.
- Вы можете использовать правила подключения Агента администрирования к Серверу администрирования, когда вы создаете правила активации профиля политики (см. раздел "Создание правила переключения Агента администрирования по сетевому местоположению" на стр. 582).

Создание профиля политики

Создание профиля доступно только для политик Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше, для политик программы Kaspersky Endpoint Security 10 Service Pack 1 для Mac, для политик плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1, для политики плагина Kaspersky Device Management для iOS.

► *Чтобы создать профиль политики, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для политики которой нужно создать профиль политики.
2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики и нажмите на кнопку **Добавить**.

   Запустится мастер создания профиля политики.
5. В окне мастера **Имя профиля политики** укажите:
   a. Имя профиля политики.

      Имя профиля не может превышать 100 символов.

   b. Состояние профиля политики (*Включен* или *Выключен*).

      Рекомендуется создавать неактивные профили политики и включать их только после полного завершения настройки параметров и условий активации профилей политики.
6. Установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, чтобы запустить мастер создания правила активации профиля политики (см. раздел "Создание правила активации профиля политики" на стр. 345). Следуйте инструкциям мастера.
7. Измените параметры профиля политики в окне свойств профиля политики, как вам необходимо (см. раздел "Изменение профиля политики" на стр. 344).
8. Сохраните изменения, нажав на кнопку **ОК**.

Профиль будет сохранен. Профиль будет активирован на устройствах, удовлетворяющих правилам активации.

Для одной политики можно создать несколько профилей политики. Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политики**. Вы можете изменить профиль политики и приоритет профиля (см. раздел "Изменение профиля политики" на стр. 344), а также удалить профиль (см. раздел "Удаление профиля политики" на стр. 345).

Изменение профиля политики

Изменение параметров профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

► *Чтобы изменить профиль политики, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно изменить профиль политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики.

   В разделе содержится список профилей, созданных для политики. Профили в списке отображаются в соответствии с их приоритетом.
5. Выберите профиль политики и нажмите на кнопку **Свойства**.
6. В окне свойств настройте параметры профиля:
   - Если необходимо, в разделе **Общие** измените имя профиля и включите или выключите профиль с помощью флажка **Включить профиль**.
   - В разделе **Правила активации** измените правила активации профиля.
   - Измените параметры политики в соответствующих разделах.
7. Нажмите на кнопку **ОК**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

Изменение приоритета профиля политики

Приоритет профилей политик определяет порядок активации профилей на клиентском устройстве. Приоритет используется, если для разных профилей политики заданы одинаковые правила активации.

Например, созданы два профиля политики: *Профиль 1* и *Профиль 2*, отличающиеся друг от друга значениями одного параметра (*Значение 1* и *Значение 2*). Приоритет *Профиля 1* выше, чем приоритет

Профиля 2. Кроме того, существуют профили с более низким приоритетом, чем *Профиль 2*. Правила активации профилей совпадают.

При выполнении правила активации будет активирован *Профиль 1*. Параметр на устройстве примет *Значение 1*. Если удалить *Профиль 1,* то *Профиль 2,* будет иметь самый высокий приоритет, и параметр примет *Значение 2*.

В списке профилей политики профили отображаются в соответствии с их приоритетом. На первом месте в списке стоит профиль с самым высоким приоритетом. Приоритет профиля можно изменять с помощью кнопок  и  .

Удаление профиля политики

► *Чтобы удалить профиль политики, выполните следующие действия:*

1. Выберите в дереве консоли группу администрирования, для которой нужно удалить профиль политики.
2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики Kaspersky Endpoint Security.
5. Выберите профиль политики, который нужно удалить, и нажмите на кнопку **Удалить**.

В результате профиль политики будет удален. Активным станет либо другой профиль политики, правила активации которого выполняются на устройстве, либо политика.

Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать правило активации профиля политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики.
5. Выберите профиль политики, для которого нужно создать правило активации, и нажмите на кнопку **Свойства**.

   В результате откроется окно свойств профиля политики.

   Если список профилей политики пуст, вы можете создать профиль политики (см. раздел "Создание профиля политики" на стр. 343).
6. Выберите раздел **Правила активации** и нажмите на кнопку **Добавить**.

В результате запустится мастер создания правила активации профиля политики.

7. В окне **Правила активации профиля политики** установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   - **Общие правила активации профиля политики**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

   - **Правила использования Active Directory**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

   - **Правила для определенного владельца устройства**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от того, кто является владельцем устройства, и от членства устройства во внутренней группе безопасности Kaspersky Security Center.

   - **Правила для характеристик оборудования**

     Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

   От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

8. В окне **Общие условия** настройте следующие параметры:

   - В поле **Устройство в автономном режиме** в раскрывающемся списке укажите условие нахождения устройства в сети:

     - **Да**

       Устройство находится во внешней сети, то есть Сервер администрирования недоступен.

     - **Нет**

       Устройство находится в сети, Сервер администрирования доступен.

     - **Значение не выбрано**

       Критерий не применяется.

   - В поле **Устройство находится в указанном сетевом местоположении** с помощью раскрывающихся списков настройте активацию профиля политики при выполнении / невыполнении на устройстве правила подключения к Серверу администрирования:

     - **Выполняется / Не выполняется**

Условие активации профиля политики (правило выполняется или не выполняется).

- **Имя правила**

  Описание сетевого местоположения устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

  Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

Окно **Общие условия** отображается, если был установлен флажок **Общие правила активации профиля политики**.

9. В окне **Условия с использованием тегов** настройте следующие параметры:

   - Список тегов

     В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

     Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

     В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

   - **Применять к устройствам без выбранных тегов**

     Установите флажок, если необходимо инвертировать выбор тегов.

     Если флажок установлен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если флажок снят, критерий не применяется. По умолчанию флажок снят.

   Окно **Условия с использованием тегов** отображается, если был установлен флажок **Общие правила активации профиля политики**.

10. В окне **Условия с использованием Active Directory** настройте следующие параметры:

    - **Членство владельца устройства в группе безопасности Active Directory**

      Если флажок установлен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

    - **Членство устройства в группе безопасности Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий

активации профиля не применяется. По умолчанию флажок снят.

- **Размещение устройства в подразделении Active Directory**

Если флажок установлен, профиль политики активируется на устройстве, которое явно или неявно входит в указанное подразделение Active Directory. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

Окно **Условия с использованием Active Directory** отображается, если был установлен флажок **Правила для использования Active Directory**.

1. В окне **Условия с использованием владельца устройства** настройте следующие параметры:

- **Владелец устройства**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "#").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Владелец устройства входит во внутреннюю группу безопасности**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "#").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- **Активировать профиль политики по наличию роли у владельца устройства**

Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца (см. раздел "Настройка прав.Роли пользователей" на стр. 646). Добавить роль вручную из списка существующих ролей.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

Окно **Условия с использованием владельца устройства** отображается, если был установлен флажок **Правила для определенного владельца устройства**.

1. В окне **Условия с использованием характеристик оборудования** настройте следующие параметры:

   - **Объем оперативной памяти (МБ)**

     Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

     - объем оперативной памяти устройства меньше указанного значения (знак "<");
     - объем оперативной памяти устройства больше указанного значения (знак ">").

     Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

   - **Количество логических процессоров**

     Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

     - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
     - количество логических процессоров устройства больше или равно указанному значению (знак ">").

     Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

   Окно **Условия с использованием характеристик оборудования** отображается, если был установлен флажок **Правила для характеристик оборудования**.

2. В окне **Имя правила активации профиля политики** в поле **Имя условия** укажите имя правила.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Правила перемещения устройств.

Размещение устройств в группах администрирования целесообразно автоматизировать при помощи

правил перемещения устройств. Правило перемещения состоит из трех основных частей: имени, условия выполнения (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила нужно снять флажок **Перемещать только устройства, не размещенные в группах администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик (на стр. 330), задачи для выборок устройств (см. раздел "Задачи" на стр. 41), назначать Агенты администрирования согласно методике (см. раздел "Настройка точек

распространения и шлюзов соединений" на стр. 534) и так далее.

Копирование правил перемещения устройств

Если вам нужно создать несколько правил перемещения устройств с аналогичными параметрами, вы можете скопировать существующее правило, а затем изменить параметры скопированного правила. Например, это удобно, когда вы должны иметь несколько одинаковых правил перемещения устройств с разными IP-диапазонами и целевыми группами.

► *Чтобы скопировать правило перемещения устройств, выполните следующие действия:*

1. Откройте главное окно программы.
2. В папке **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   Откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** выберите правило перемещения устройств, которое вы хотите скопировать.
4. Нажмите на кнопку **Копировать**.

Копия выбранного правила будет добавлена в конец списка.

Новое правило будет создано выключенным. Вы можете выключить или изменить правило в любое время.

Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для программ, не подпадающих ни под одну KL-категорию (например, для программ, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива программы (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Нельзя создавать автоматически обновляемые категории программного обеспечения на основе папок Мои документы, %windir%, %ProgramFiles%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

Необходимые условия для установки программ на устройства организации-клиента

Процесс удаленной установки программ на устройства организации-клиента совпадает с процессом удаленной установки программ внутри организации (см. раздел "Программы "Лаборатории Касперского". Централизованное развертывание" на стр. 271).

Для установки программ на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой программ на устройства организации-клиента требуется установить на них Агент администрирования.

  При настройке инсталляционного пакета Агента администрирования поставщиком услуг в программе Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

  - В разделе **Подключение** в строке **Адрес Сервера** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на точку распространения.
  - В разделе **Дополнительно** требуется установить флажок **Подключаться к Серверу администрирования через шлюз соединений**. В строке **Адрес шлюза соединений** нужно указать адрес точки распространения. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.
- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью точек распространения**. Выбор способа загрузки осуществляется следующим образом:
  - При установке программ с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:
    - при создании задачи удаленной установки в окне **Параметры**;
    - в окне свойств задачи удаленной установки в разделе **Параметры**.
  - При установке программ с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.
- Учетная запись, под которой работает точка распространения, должна иметь доступ к ресурсу Admin$ на клиентских устройствах.

Просмотр и изменение локальных параметров программы

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами программ на устройствах через Консоль администрирования.

Локальные параметры программы – это параметры программы, индивидуальные для устройства. С помощью Kaspersky Security Center вы можете устанавливать локальные параметры программ для устройств, входящих в группы администрирования.

Подробные описания параметров программ "Лаборатории Касперского" приводятся в Руководствах для этих программ.

► *Чтобы просмотреть или изменить локальные параметры программы, выполните следующие действия:*

1. В рабочей области группы, в которую входит нужное вам устройство, выберите закладку **Устройства**.
2. В окне свойств в разделе **Программы** выберите соответствующую программу.
3. Откройте окно свойств программы двойным щелчком мыши по названию программы или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранной программы, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт замком ( ) в политике).

Обновление Kaspersky Security Center и управляемых программ

В этом разделе описаны шаги, которые необходимо выполнить для обновления Kaspersky Security Center и управляемых программ.

В этом разделе

Сценарий: Обновление Kaspersky Security Center и управляемых программ

В этом разделе описан основной сценарий обновления программы Kaspersky Security Center.

Сценарий развертывания Kaspersky Security Center состоит из следующих шагов:

a. **Планирование ресурсов**

Убедитесь, что на жестком диске имеется достаточно свободного места для создания резервной копии данных Сервера администрирования.

b. **Получение файла установки Kaspersky Security Center**

   Получите исполняемый файл для текущей версии Kaspersky Security Center и сохраните его на устройство, выполняющее роль Сервера администрирования. Ознакомьтесь с Информацией о выпуске для Kaspersky Security Center.

c. **Создание резервной копии предыдущей версии**

   С помощью утилиты резервного копирования и восстановления данных создайте резервную копию данных Сервера администрирования (см. раздел "Утилита резервного копирования и восстановления данных (klbackup)" на стр. 565).

d. **Запуск установщика**

   Запустите исполняемый файл для версии 11 (см. раздел "Выборочная установка" на стр. 190). После запуска файла укажите, что была создана резервная копия, а также путь к ней. Будет выполнено восстановление данных из резервной копии.

e. **Обновление управляемых программ**

   Можно обновить программу, если доступна новая версия. Убедитесь, что текущая версия Kaspersky Security Center совместима с этой программой. Затем обновите программу, как описано в информации о выпуске.

См. также:

Порты, используемые Kaspersky Security Center 56

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения 61

Основные понятия..... 33

Архитектура программы..... 48

Об обновлении баз, программных модулей и программ "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вы должны своевременно предоставлять обновления:

- баз и программных модулей "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

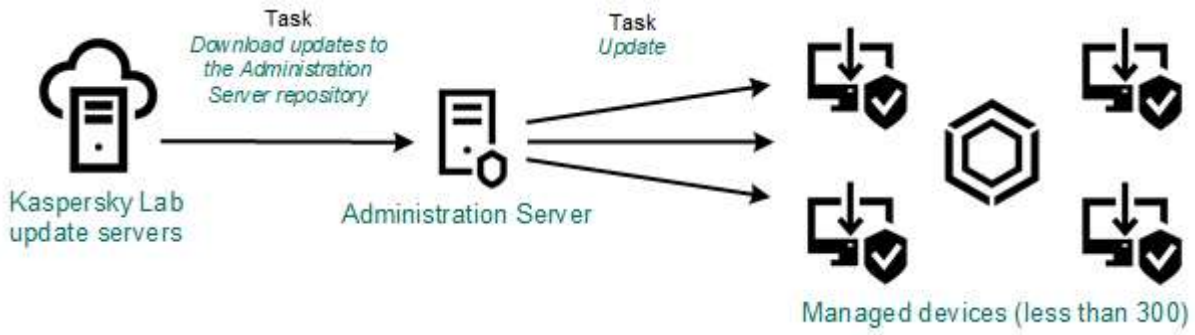
В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- Использование задачи Загрузка обновлений в хранилище Сервера администрирования

- Использование двух задач:
  - задача Загрузка обновлений в хранилище Сервера администрирования;
  - задача Загрузки обновлений в хранилища точек распространения.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security для Windows на управляемых устройствах

Использование задачи Загрузка обновлений в хранилище Сервера администрирования

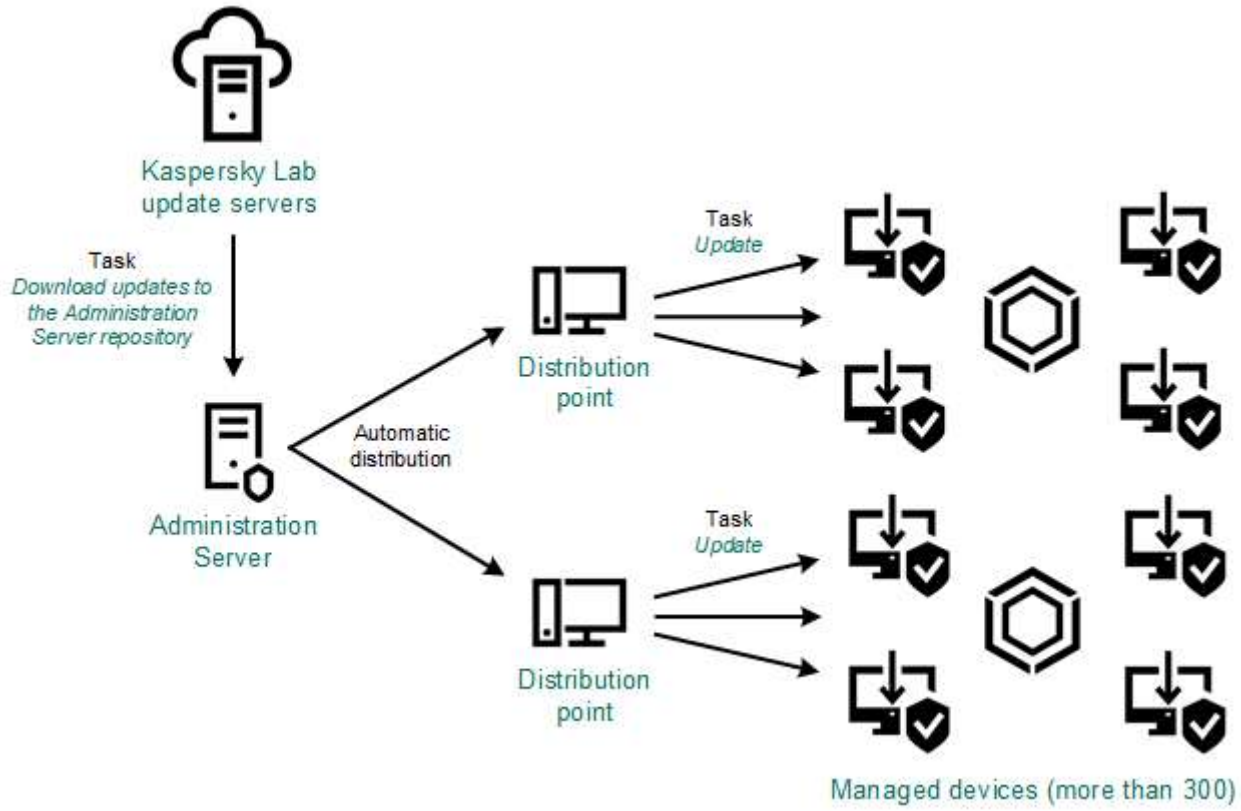
В этой схеме Kaspersky Security Center загружает обновления с помощью задачи Загрузка обновлений в хранилище Сервера администрирования (см. рисунок ниже). В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).



По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения (см. раздел "О точках распространения" на стр. 86) для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 88).

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.



После завершения задачи Загрузка обновлений в хранилище Сервера администрирования следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и программные модули "Лаборатории Касперского" для Kaspersky Security Center.

  Эти обновления устанавливаются автоматически.

- Базы и программные модули "Лаборатории Касперского" для программ безопасности на управляемых устройствах.

  Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows.

- Обновления для Сервера администрирования.

  Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

  > Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

  По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования.

- Обновления для программ безопасности.

  По умолчанию программа Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. Обновления устанавливаются с помощью задачи Обновление и могут быть настроены в свойствах этой задачи.

Задача Загрузка обновлений в хранилище Сервера администрирования недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

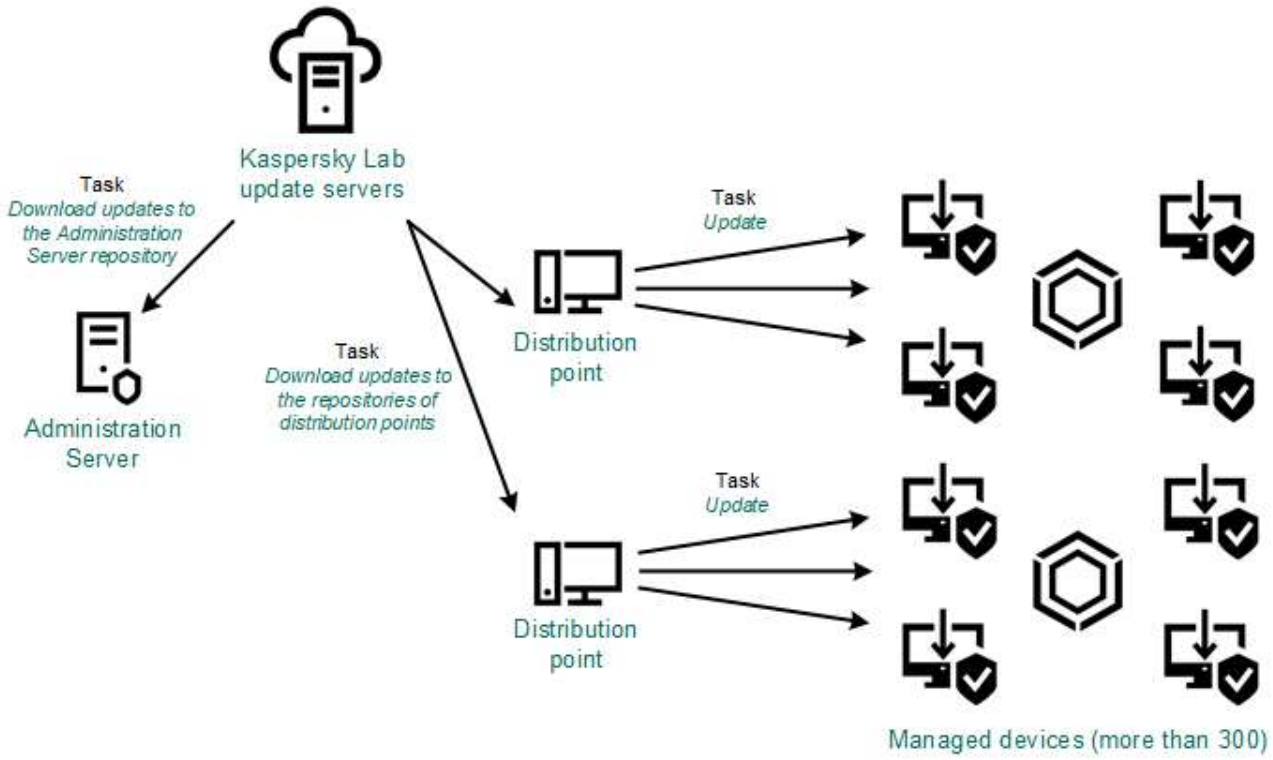
Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются программами. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи Загрузка обновлений в хранилище, для обеспечения загрузки необходимых версий баз и программных модулей "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия программы;
- идентификатор установки программы;
- идентификатор активного ключа;
- идентификатор запуска задачи Загрузка обновлений в хранилище Сервера администрирования.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и / или точки распространения на использование протокола HTTP вместо HTTPS.

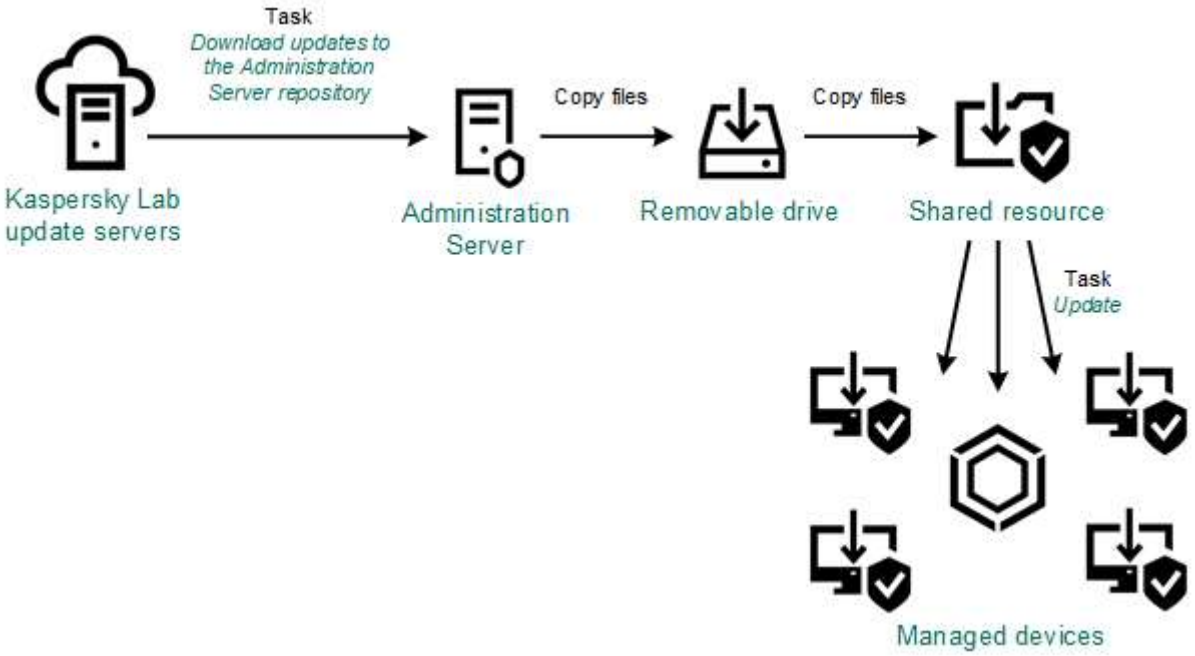
Для реализации этой схемы создайте задачу Загрузка обновлений в хранилища точек распространения в дополнение к задаче Загрузка обновлений хранилища Сервера администрирования. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Для этой схемы также требуется задача Загрузка обновлений в хранилище Сервера администрирования, так как эта задача используется для загрузки баз и программных модулей "Лаборатории Касперского" для

Kaspersky Security Center.

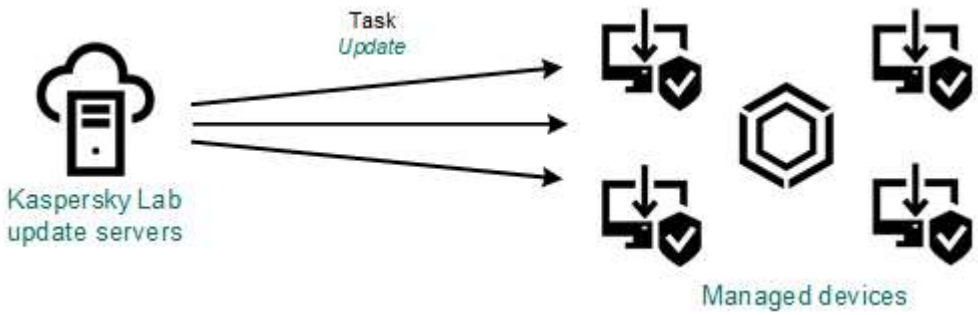
Вручную через локальную папку, общую папку или FTP-сервер

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, программных модулей и программ "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в настройках Kaspersky Endpoint Security для Windows (см. рисунок ниже).



Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security для Windows на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security для Windows на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



В этой схеме программы безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе программы безопасности. Полное описание этих параметров приведено в документации Kaspersky

Endpoint Security для Windows.

Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"

Когда Kaspersky Security Center загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и программных модулей. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и программных модулей.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Функция загрузки файлов различий может быть включена только на Серверах администрирования и точках распространения версии 11 и выше. Чтобы сохранить файлы различий на Серверах администрирования и точках распространения предыдущих версий, их необходимо обновить до версии 11.
Функция загрузки файлов различий несовместима с офлайн-моделью получения обновлений (см. стр. 438). Это означает, что Агенты администрирования, использующие офлайн-модель загрузки обновлений, не загружают файлы различий, даже если функция загрузки файлов различий включена на Сервере администрирования или точке распространения, которые предоставляют обновления этим Агентам администрирования.
Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Сценарий включения функции загрузки файлов различий

Необходимые предварительные условия для сценария:

- Сервер администрирования и точки распространения обновлены до версии 11.
- Офлайн модель получения обновлений выключена в свойствах политики Агента администрирования.

Сценарий включения функции загрузки файлов различий состоит из следующих шагов:

a. **Включить функцию на Сервере администрирования.**

   Функция включена в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования (см. раздел "Параметры задачи загрузки обновлений в хранилище Сервера администрирования" на стр. 887).

b. **Включить функцию для точки распространения, которая получает обновления с помощью задачи Загрузка обновлений в хранилища точек распространения.**

   Функция включена в свойствах задачи (см. раздел "Параметры задачи загрузки обновлений в хранилища точек распространения" на стр. 889).

c. **Включить функцию для точки распространения, которая получает обновления с Сервера администрирования.**

   Эта функция включается в свойствах политики Агента администрирования (см. стр. 624) и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования (см. раздел "Загрузка обновлений точками распространения" на стр. 383). в разделе **Точки распространения**.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Задача загрузки обновлений в хранилище Сервера администрирования создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования может быть создана в одном экземпляре. Поэтому вы можете создать задачу загрузки обновлений в хранилище Сервера администрирования только в случае, если она была удалена из списка задач Сервера администрирования.

► *Чтобы создать задачу загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню **Задачи** в дереве консоли выберите пункт **Создать** → **Задачу**.
   - В рабочей области папки **Категории программ** нажмите на кнопку **Создать категорию**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В окне мастера **Выбор типа задачи** выберите **Загрузка обновлений в хранилище Сервера администрирования**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
   - **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского".

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.

- Главный Сервер администрирования.

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

  - **Прочие параметры**:
    - **Форсировать обновление подчиненных Серверов**

Если флажок установлен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

По умолчанию параметр выключен.

- **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступа к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений

"Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не форсировать обновление устройств и подчиненных Серверов администрирования до окончания копирования**

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

- **Обновлять модули Агентов администрирования**

Если этот параметр включен, обновления для программных модулей Агента администрирования устанавливаются автоматически после того, как Сервер администрирования завершит выполнение задачи Загрузка обновлений в хранилище и обновления будут загружены в хранилище. Полученные обновления модулей Агента администрирования можно установить вручную.

По умолчанию параметр включен.

1. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный

день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

- антивирусы для рабочих станций и файловых серверов;
- антивирусы защиты периметра;
- антивирусы для почтовых систем.

По умолчанию выбраны все типы программ.

Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по

расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище Сервера администрирования** появится в рабочей области списка задач Сервера администрирования.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи Загрузка обновлений в хранилище Сервера администрирования обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

См. также:

Проверка полученных обновлений.....373

Параметры задачи загрузки обновлений в хранилище Сервера администрирования 887

Создание задачи загрузки обновлений в хранилища точек распространения

Создание задачи загрузки обновлений в хранилища точек распространения доступно только для устройств под управлением Windows.

Вы можете создать задачу Загрузка обновлений в хранилища точек распространения для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

► *Чтобы создать задачу загрузки обновлений в хранилища точек распространения для выбранной группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Создать задачу** в рабочей области папки запустите мастер создания задачи.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center 11**, раскройте папку **Дополнительно** и выберите задачу **Загрузка обновлений в хранилища точек распространения**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
   - **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского".

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.
- Главный Сервер администрирования.

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть

FTP-сервером, HTTP-сервером или общим ресурсом SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Прочие параметры**:
  - **Папка для хранения обновлений**

Папка используется только для загрузки обновлений. Укажите локальную папку на устройствах, которые назначены точками распространения. Вы можете использовать системные переменные.

1. В окне мастера **Выберите группу администрирования** нажмите на кнопку **Обзор** и выберите группу администрирования, для которой задача будет применена.
2. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:
   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилища точек распространения** появится в списке задач Агента администрирования в соответствующей группе администрирования и в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи загрузки обновлений в хранилища точек распространения обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

В окне свойств Сервера администрирования выберите раздел **Точки распространения**. В свойствах каждой точки распространения в разделе **Источники обновлений** можно указать источники обновлений (**Получать с Сервера администрирования** или **Использовать задачу принудительной загрузки обновлений**). Для точки распространения, назначенной вручную или автоматически, по умолчанию выбран вариант **Получать с Сервера администрирования**. Такие точки распространения будут использовать результаты задачи загрузки обновлений в хранилища точек распространения.

В свойствах каждой точки распространения указана сетевая папка, настроенная индивидуально для этой точки распространения. Названия папок могут быть разными для разных точек распространения. Поэтому не рекомендуется изменять сетевую папку обновлений в свойствах задачи, если задача создается для группы устройств.

Вы можете изменить сетевую папку обновлений в свойствах задачи загрузки обновлений в хранилища точек распространения, если вы создаете локальную задачу для устройства.

Предыдущие версии программы, Kaspersky Security Center 10 Service Pack 2 и ниже, позволяли создать задачу загрузки обновлений для точек распространения только как локальную задачу. Начиная с версии Kaspersky Security Center 10 Service Pack 3 такого ограничения нет, что приводит к уменьшению трафика.

См. также:

Параметры задачи загрузки обновлений в хранилища точек распространения 889

Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования

► *Чтобы настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:*

1. В рабочей области папки дерева консоли **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

Откроется окно свойств задачи Загрузка обновлений в хранилище Сервера администрирования. В нем вы можете настроить параметры загрузки обновлений в хранилище Сервера администрирования.

См. также:

Параметры задачи загрузки обновлений в хранилище Сервера администрирования..... 887

Проверка полученных обновлений

► *Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства, выполните следующие действия:*

1. В рабочей области папки **Задачи** дерева консоли выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.
3. В открывшемся окне свойств задачи в разделе **Проверка обновлений** установите флажок **Выполнять проверку обновлений перед распространением** и выберите задачу проверки обновлений одним из следующих способов:
   - Нажмите на кнопку **Обзор**, чтобы выбрать уже сформированную задачу проверки обновлений.

- Нажмите на кнопку **Создать**, чтобы создать задачу проверки обновлений.

  В результате запустится мастер создания задачи проверки обновлений. Следуйте далее указаниям мастера.

  Во время создания задачи проверки обновлений необходимо выбрать группу администрирования, на устройствах которой будет выполняться задача. Устройства, входящие в эту группу, называются *тестовыми устройствами*.

  > В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Это позволяет повысить качество проверки, снизить риск возникновения ложных срабатываний, а также вероятность обнаружения вирусов при проверке. При нахождении вирусов на тестовых устройствах задача проверки обновлений считается завершившейся неудачно.

4. Закройте окно свойств задачи загрузки обновлений в хранилище Сервера администрирования, нажав на кнопку **ОК**.

В результате в рамках выполнения задачи загрузки обновлений в хранилище Сервера администрирования будет выполняться задача проверки полученных обновлений. Сервер администрирования будет копировать обновления с источника, сохранять их во временном хранилище и запускать задачу проверки обновлений. В случае успешного выполнения этой задачи обновления будут скопированы из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates). Обновления распространятся на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи проверки обновлений размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции будут выполнены при следующем запуске задачи загрузки обновлений в хранилище Сервера администрирования, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты программы безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача проверки обновлений считается успешно выполненной.

Настройка проверочных политик и вспомогательных задач

При создании задачи проверки обновлений Сервер администрирования формирует проверочные политики, а также вспомогательные групповые задачи обновления и проверки по требованию.

На выполнение вспомогательных групповых задач обновления и проверки по требованию требуется некоторое время. Эти задачи выполняются в рамках выполнения задачи проверки обновлений. Задача проверки обновлений выполняется в рамках выполнения задачи загрузки обновлений в хранилище. Время выполнения задачи загрузки обновлений в хранилище включает в себя время выполнения вспомогательных групповых задач обновления и проверки по требованию.

Параметры проверочных политик и вспомогательных задач можно изменять.

► *Чтобы изменить параметры проверочной политики или вспомогательной задачи, выполните следующие действия:*

1. В дереве консоли выберите группу, для которой сформирована задача проверки обновлений.
2. В рабочей области группы выберите одну из следующих закладок:
   - **Политики**, если вы хотите изменить параметры проверочной политики.
   - **Задачи**, если вы хотите изменить параметры вспомогательной задачи.
3. В рабочей области закладки выберите политику или задачу, параметры которой вы хотите изменить.
4. Откройте окно свойств этой политики (задачи) одним из следующих способов:
   - В контекстном меню политики (задачи) выберите пункт **Свойства**.
   - По ссылке **Настроить параметры политики** (**Настроить параметры задачи**) в блоке работы с выбранной политикой (задачей).

Чтобы проверка обновлений выполнялась правильно, необходимо соблюдать следующие ограничения на изменение параметров проверочных политик и вспомогательных задач:

- В параметрах вспомогательных задач:
  - Сохранять на Сервере администрирования все события с уровнями важности **Критическое событие** и **Отказ функционирования**. На основе событий этих типов Сервер администрирования проводит анализ работы программ.
  - Использовать в качестве источника обновлений Сервер администрирования.
  - Указывать тип расписания задач: **Вручную**.
- В параметрах проверочных политик:
  - Не использовать технологии ускорения проверки iChecker, iSwift и iStream.
  - Выбрать действия над зараженными объектами: **Не запрашивать** / **Пропустить** / **Записывать**

информацию в отчет.

- В параметрах проверочных политик и вспомогательных задач:

  Если после установки обновлений программных модулей потребуется перезагрузка устройства, ее следует выполнить незамедлительно. Если устройство не будет перезагружено, то проверить этот тип обновлений будет невозможно. Для некоторых программ установка обновлений, требующих перезагрузки, может быть запрещена или выполняться только после подтверждения от пользователя. Эти ограничения должны быть отключены в параметрах проверочных политик и вспомогательных задач.

Просмотр полученных обновлений

► *Чтобы просмотреть список полученных обновлений,*

в дереве консоли в папке **Хранилища** выберите вложенную папку **Обновления и патчи ПО "Лаборатории Касперского"**.

В рабочей области папки **Обновления и патчи ПО "Лаборатории Касперского"** представлен список обновлений, сохраненных на Сервере администрирования.

Автоматическое распространение обновлений

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления на клиентские устройства и подчиненные Серверы администрирования.

В этом разделе

Автоматическое распространение обновлений на клиентские устройства

► *Чтобы обновления выбранной вами программы автоматически распространялись на клиентские устройства сразу после загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские устройства.
2. Создайте задачу распространения обновлений этой программы для выбранных клиентских устройств одним из следующих способов:
   - Если требуется распространять обновления на клиентские устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание групповой задачи" на стр. 318).
   - Если требуется распространять обновления на клиентские устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. 320).

   Запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

   a. В окне мастера **Тип задачи** в узле нужной вам программы выберите задачу распространения обновлений.

      Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от программы, для которой создается задача. Подробнее о названиях задач обновления для выбранных программ "Лаборатории Касперского" см. в Руководствах к этим программам.

   b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

   В результате созданная задача распространения обновлений будет запускаться для выбранных устройств каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужной вам программы уже создана для выбранных устройств, для автоматического распространения обновлений на клиентские устройства в окне свойств задачи в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

Автоматическое распространение обновлений на подчиненные Серверы администрирования

► *Чтобы обновления выбранной вами программы автоматически распространялись на подчиненные Серверы администрирования сразу после загрузки обновлений в хранилище главного Сервера администрирования, выполните следующие действия:*

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.
3. Откройте раздел **Параметры** окна свойств выбранной задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В разделе **Параметры** окна свойств задачи откройте окно **Прочие параметры** по ссылке **Настроить** в подразделе Прочие параметры.
5. В открывшемся окне **Прочие параметры** установите флажок **Форсировать обновление подчиненных Серверов**.

В параметрах задачи получения обновлений Сервером администрирования на закладке **Параметры** окна свойств задачи установите флажок **Форсировать обновление подчиненных Серверов**.

В результате сразу после получения обновлений главным Сервером администрирования будут автоматически запускаться задачи загрузки обновлений подчиненными Серверами администрирования, независимо от расписания, установленного в параметрах этих задач.

Автоматическая установка обновлений программных модулей Агентов администрирования

► *Чтобы обновления программных модулей Агентов администрирования автоматически устанавливались после их загрузки в хранилище Сервера администрирования, выполните следующие действия:*

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.
3. Откройте окно свойств выбранной задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.
4. В окне свойств задачи выберите раздел **Параметры**.
5. По ссылке **Настроить** в блоке **Прочие параметры** откройте окно **Прочие параметры**.
6. В открывшемся окне **Прочие параметры** установите флажок **Обновлять модули Агентов**

администрирования.

Если флажок установлен, обновления программных модулей Агента администрирования будут устанавливаться автоматически после их загрузки в хранилище Сервера администрирования. Если флажок снят, автоматическая установка обновлений Агента администрирования не выполняется. Полученные обновления можно устанавливать вручную. По умолчанию флажок установлен.

> Автоматическая установка программных модулей Агентов администрирования доступна только для Агентов администрирования версии 10 Service Pack 1 и ниже.

7. Нажмите на кнопку **ОК**.

В результате обновления программных модулей Агентов администрирования будут устанавливаться автоматически.

Назначение устройства точкой распространения вручную

Kaspersky Security Center позволяет назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 88).

Устройства, выполняющие роль точек распространения, должны быть защищены от любого типа несанкционированного доступа, в том числе физически защищены.

► *Чтобы вручную назначить устройство точкой распространения, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** нажмите на кнопку **Добавить**. Кнопка доступна, если выбран вариант **Вручную назначать точки распространения**.

   Откроется окно **Добавление точки распространения**.
4. В окне **Добавление точки распространения** выполните следующие действия:
   a. Выберите устройство, которое будет выполнять роль точки распространения (в группе администрирования или укажите IP-адрес устройства). При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения (см. стр. 44).
   b. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

5. Нажмите на кнопку **ОК**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

6. Выберите в списке добавленную точку распространения и по кнопке **Свойства** откройте окно ее свойств.

7. В окне свойств настройте параметры точки распространения:

   - В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами:

     - **Номер SSL-порта**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.

     - **Использовать многоадресную IP-рассылку**

       Если флажок установлен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

     - **Адрес IP-рассылки**

       IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

       По умолчанию указан IP-адрес 225.6.7.8.

     - **Номер порта IP-рассылки**

       Номер порта многоадресной рассылки.

       Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

     - **Распространять обновления**

       Если флажок установлен, обновления распространяются на клиентские устройства с помощью этой точки распространения.

       По умолчанию флажок установлен.

     - **Распространять инсталляционные пакеты**

       Если флажок установлен, инсталляционные пакеты обновления распространяются на клиентские устройства с помощью этой точки распространения.

       По умолчанию флажок установлен.

   - В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и / или сетевое местоположение).

- В разделе **Прокси-сервер KSN** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.
  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. 736).

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.
  - **Переслать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

    По умолчанию параметр включен.
  - **Доступ к облачной-службе KSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN.

  - **TCP-порт**

    Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.
  - **UDP-порт**.

    Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию флажок снят, подключение к прокси-серверу KSN выполняется через UDP-порт 15111.
- В разделе **Обнаружение устройств** настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения.
  - **Windows-домены**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.
  - **Active Directory**

Вы можете включить опрос Active Directory и задать расписание опроса.

Если вы установили флажок **Разрешить опрос сети**, выберите один из следующих вариантов:

- **Опросить текущий домен Active Directory**.
- **Опросить лес доменов Active Directory**.
- **Опросить указанные домены Active Directory**. Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.

- **IP-диапазоны**

  Вы можете включить обнаружение устройств для IP-диапазонов.

  Если вы установили флажок **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса.

  Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов (см. раздел "Добавление IP-диапазонов в список опрашиваемых диапазонов точки распространения" на стр. 539).

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.

  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

В результате выбранные устройства будут выполнять роль точек распространения.

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

► *Чтобы назначить точки распространения автоматически с помощью Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите вариант

Автоматически назначать точки распространения.

> Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Удаление устройства из списка точек распространения

► *Чтобы удалить устройство из списка точек распространения, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите устройство, выполняющее функции точки распространения, и нажмите на кнопку **Удалить**.

В результате устройство будет удалено из списка точек распространения и перестанет выполнять функции точки распространения.

> Нельзя удалить устройство из списка точек распространения, если оно было назначено Сервером администрирования автоматически (см. раздел "Назначение устройства точкой распространения вручную" на стр. 379).

Загрузка обновлений точками распространения

Kaspersky Security Center позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

► *Чтобы настроить получение обновлений для точки распространения, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите точку распространения, через которую обновления будут доставляться на клиентские устройства группы.
4. По кнопке **Свойства** откройте окно свойств выбранной точки распространения.

5. В окне свойств точки распространения выберите раздел **Источник обновлений**.
6. Выберите источник обновлений для точки распространения:
    - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получать с Сервера администрирования**:
        - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. раздел "Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"" на стр. 361).

По умолчанию параметр включен.

- Чтобы точка распространения получала обновления с помощью задачи, выберите вариант **Использовать задачу принудительной загрузки обновлений**:
    - Нажмите на кнопку **Выбрать**, если такая задача уже есть на устройстве, и выберите задачу в появившемся списке.
    - Нажмите на кнопку **Новая задача**, чтобы создать задачу, если такой задачи еще нет на устройстве. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

    Задача загрузки обновлений в хранилища точек распространения является локальной. Для каждого устройства, выполняющего роль точки распространения, задачу требуется создавать отдельно.

В результате точка распространения будет получать обновления из указанного источника.

Удаление обновлений программного обеспечения из хранилища

► *Чтобы удалить обновления программного обеспечения из хранилища Сервера администрирования, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** выберите обновление, которое нужно удалить.
3. В контекстном меню обновления выберите **Удалить файлы обновлений**.

Обновления программного обеспечения будут удалены из хранилища Сервера администрирования.

Алгоритм установки патча для программы "Лаборатории Касперского" в кластерной модели

Kaspersky Security Center поддерживает только ручную установку патчей для программ "Лаборатории Касперского" в кластерной модели.

Чтобы установить патч для программы "Лаборатории Касперского", выполните следующие действия:

1. Загрузите на каждый узел кластера патч.
2. Запустите установку патча на активном узле.

   Дождитесь успешной установки патча.
3. Последовательно запустите патч на всех подчиненных узлах кластера.

   При запуске патча из командной строки используйте ключ "`-CLUSTER_SECONDARY_NODE`".

   В результате этих действий патч будет установлен на каждом узле кластера.
4. Запустите вручную кластерные службы "Лаборатории Касперского".

Каждый узел кластера будет отображаться в Консоли администрирования как устройство с установленным Агентом администрирования.

Информацию об установленных патчах можно просмотреть в папке **Обновления программного обеспечения** или в отчете о версиях обновлений программных модулей программ "Лаборатории Касперского".

См. также:

Настройка общих параметров Сервера администрирования 556

Управление программами на клиентских устройствах

Kaspersky Security Center позволяет управлять программами "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах.

Администратор может выполнять следующие действия:

- создавать категории программ на основании заданных критериев;
- управлять категориями программ с помощью специально созданных правил;
- управлять запуском программ на устройствах;
- выполнять инвентаризацию и вести реестр программного обеспечения, установленного на устройствах;
- закрывать уязвимости программного обеспечения, установленного на устройствах;
- устанавливать обновления Windows Update и других производителей программного обеспечения

на устройствах;

- отслеживать использование ключей для групп лицензионных программ.

В этом разделе

Группы программ

В этом разделе описана работа с группами программ, установленных на устройствах.

Создание категорий программ

Kaspersky Security Center позволяет создавать категории программ, установленных на устройствах.

Категории программ можно создавать следующими способами:

- Администратор указывает папку, исполняемые файлы из которой попадают в выбранную категорию.
- Администратор указывает устройство, исполняемые файлы с которого попадают в выбранную категорию.
- Администратор задает критерии, по которым программы попадают в выбранную категорию.

Когда категория программ создана, администратор может задать правила для этой категории программ. Правила определяют поведение программ, входящих в указанную категорию. Например, можно запретить или разрешить запуск программ, входящих в категорию.

Управление запуском программ на устройствах

Kaspersky Security Center позволяет управлять запуском программ на устройствах в режиме "Белый список". Подробное описание приведено в онлайн-справке Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.1.0/ru-RU/127971.htm. В режиме "Белый список" на выбранных устройствах разрешен запуск только тех программ, которые входят в указанные категории. Администратор может просматривать результаты статического анализа правил запуска программ на устройствах по каждому пользователю.

Инвентаризация программного обеспечения, установленного на устройствах

Kaspersky Security Center позволяет выполнять инвентаризацию программного обеспечения на устройствах под управлением Windows. Агент администрирования получает информацию обо всех программах, установленных на устройствах. Информация, полученная в результате инвентаризации, отображается в рабочей области папки **Реестр программ**. Администратор может просматривать подробную информацию о каждой программе, в том числе версию и производителя.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Управление группами лицензионных программ

Kaspersky Security Center позволяет создавать группы лицензионных программ. В группу лицензионных программ входят программы, отвечающие критериям, заданным администратором. Администратор может указывать следующие критерии для групп лицензионных программ:

- название программы;
- версия программы;
- производитель;
- тег программы.

Программы, соответствующие одному или нескольким критериям, автоматически попадают в группу. Для создания группы лицензионных программ должен быть задан хотя бы один критерий включения программ в эту группу.

Каждая группа лицензионных программ имеет свой ключ. Ключ группы лицензионных программ определяет допустимое количество установок для программ, входящих в группу. Если количество установок превысило заданное в ключе ограничение, на Сервере администрирования регистрируется информационное событие. Администратор может указать дату окончания действия ключа. При наступлении этой даты на Сервере администрирования регистрируется информационное событие.

Просмотр информации об исполняемых файлах

Kaspersky Security Center получает всю информацию об исполняемых файлах, которые запускались на устройствах с момента установки на них операционной системы. Полученная информация об исполняемых файлах отображается в главном окне программы в рабочей области папки **Исполняемые файлы**.

В этом разделе

Создание категорий программ

► *Чтобы создать категорию программ, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Категории программ**.
2. По кнопке **Создать категорию** запустите мастер создания пользовательской категории.
3. В окне мастера выберите тип пользовательской категории:
   - **Пополняемая вручную категория**. Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
   - **Автоматически пополняемая категория**. Укажите папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию.

     При создании автоматически пополняемой категории программа выполняет инвентаризацию следующих форматов файлов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Укажите устройство., исполняемые файлы которого должны попадать попадать в категорию автоматически.
4. Следуйте указаниям мастера.

В результате работы мастера создается пользовательская категория программ. Просмотреть созданные категории можно в списке категорий в рабочей области папки **Категории программ**.

Категории программ используются компонентом Контроль программ, который входит в состав программы защиты Kaspersky Endpoint Security для Windows. Компонент Контроль программ позволяет администратору установить ограничения на запуск программ на клиентских устройствах, например, на основании программ, которые входят в выбранную категорию.

Создание пополняемой вручную категории программ

► *Чтобы создать пополняемую вручную категорию программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. Нажмите на кнопку **Создать категорию**.

   Запустится мастер создания категории.
3. В окне мастера выберите тип пользовательской категории **Пополняемая вручную категория**.
4. В окне **Настройка условий для включения программ в категорию** нажмите на кнопку **Добавить**.
5. В раскрывающемся списке задайте необходимые вам параметры:

   - **Из списка исполняемых файлов**

     Если выбран этот вариант, программы для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

   - **Из свойств файла**

     Если выбран этот вариант, можно вручную указать детальные данные исполняемых файлов, которые будут добавлены в пользовательскую категорию программ.

   - **Метаданные файлов папки**

     Укажите папку на клиентском устройстве, которая содержит исполняемые файлы. Метаданные исполняемых файлов, входящих в указанную папку, будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

   - **Хеши файлов папки**

     Если выбран этот вариант, можно выбрать или создать папку на клиентском устройстве. Хеш файлов, содержащихся в указанной папке, будет передаваться на Сервер администрирования. Программы, имеющие такой же хеш, как и файлы в указанной папке, будут добавлены в пользовательскую категорию программ.

   - **Сертификаты файлов из папки**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты

исполняемых файлов считываются и добавляются в условия категории. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Метаданные файлов установщика MSI**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика программы будут передаваться на Сервер администрирования. Программы, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию программ.

- **Контрольные суммы файлов msi-инсталлятора программы**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Хеш файлов установщика программы будет передаваться на Сервер администрирования. Программы, у которых хеш файлов установщика MSI совпадает с указанным, будут добавлены в пользовательскую категорию программ.

- **KL-категория**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать категорию программ "Лаборатории Касперского". Программы, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию программ.

- **Папка программы**

  Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию программ.

- **Сертификаты из хранилища сертификатов**

  Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Тип носителя**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск программы. Программы, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию программ.

6. Следуйте далее указаниям мастера.

Kaspersky Security Center работает с метаданными только из тех файлов, которые содержат цифровую подпись. Невозможно создать категорию на основе метаданных файлов, не содержащих цифровой подписи.

В результате работы мастера будет создана пользовательская категория программ, пополняемая вручную. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

Создание автоматически пополняемой категории программ

► *Чтобы создать автоматически пополняемую категорию программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. По кнопке **Новая категория** запустите мастер создания пользовательской категории.

   В окне мастера выберите тип пользовательской категории **Автоматически пополняемая категория**.
3. В окне **Папка хранилища** задайте необходимые вам параметры:
   - Путь к папке автоматического пополнения категории

     В поле укажите путь к папке, в которой Сервер администрирования будет периодически искать исполняемые файлы. Путь к папке задается в момент создания категории. Изменить путь к папке нельзя.
   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию программ включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль программ регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.
   - **Включать в категорию данные о скриптах**

     В категорию программ включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.
   - Алгоритм вычисления хеш-функции

     В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение

хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии программ безопасности Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии программ безопасности ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии программы безопасности Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если флажок установлен, программа периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если флажок снят, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

По умолчанию флажок снят.

- **Период проверки (ч)**

  В поле можно указать интервал времени в часах, по истечении которого программа принудительно проверяет на наличие изменений папку автоматического пополнения категории. По умолчанию период принудительной проверки равен 24 часам. Поле доступно, если установлен флажок **Принудительно проверять папку на наличие изменений**.

  По умолчанию флажок снят.

4. Следуйте далее указаниям мастера.

В результате работы мастера будет создана автоматически пополняемая категория программ. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

Добавление исполняемых файлов, связанных с событием, в категорию программы

События типа **Запуск программы запрещен** и **Запуск программы запрещен в тестовом режиме** можно добавлять в существующую категорию программ, пополняемую вручную, или в новую категорию программ.

► *Чтобы добавить исполняемые файлы, связанные событиями компонента Контроль программ, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. На закладке **События** выберите нужное вам событие.
4. В контекстном меню события выберите пункт **Добавить в категорию**.
5. В окне **Выберите категорию программ** настройте необходимые вам параметры:

   Выберите один из следующих вариантов:

   - **Создать категорию программ**

     Выберите этот вариант, если необходимо создать новую категорию программ.

     Нажмите на кнопку **ОК**, чтобы запустить мастер создания пользовательской категории. В результате работы мастера будет создана категория с указанными параметрами.

     По умолчанию вариант не выбран.

   - **Добавить правила в указанную категорию**

     Выберите этот вариант, если необходимо добавить правила в существующую

категорию программ. Выберите необходимую категорию в списке категорий программ.

По умолчанию этот вариант выбран.

В блоке **Тип правила** выберите параметры:

- **Добавить в категорию**

  Выберите этот вариант, если необходимо добавить правила в условия категории программ.

  По умолчанию этот вариант выбран.

- **Исключить из категории**

  Выберите этот вариант, если необходимо добавить правила в исключения категории программ.

В блоке **Тип информации о файле** выберите один из параметров:

- **Данные сертификата или SHA-256 для файлов без сертификата**

  Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

  Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

  Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

  По умолчанию этот вариант выбран.

- **Данные сертификата (файлы без сертификата пропускаются)**

  Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

  Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA-256 (файлы без SHA-256 пропускаются)**

  Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе

хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**

  Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

6. Нажмите на кнопку **ОК**.

Настройка управления запуском программ на клиентских устройствах

Категоризация программ позволяет оптимизировать процесс управления запуском программ на устройствах. Вы можете создать категорию программ и настроить компонент Контроль программ политики так, что на устройствах, на которых применена эта политика, будут запускаться только программы из указанной категории. Например, вы создали категорию, которая содержит программы *Программа_1* и *Программа_2*. После добавления этой категории в политику, на устройствах, к которым применена эта политика, будет разрешен запуск только двух программ, *Программа_1* и *Программа_2*. Если пользователь попытается запустить программу, которая не входит в категорию, например, *Программу_3*, то запуск такой программы будет заблокирован. Пользователю будет отображено сообщение о том, что запуск *Программы_3* запрещен в соответствии с правилом Контроля программ. Вы можете создать автоматически пополняемую категорию на основе различных критериев, входящих в указанную папку. В этом случае файлы будут автоматически добавляться в категорию из указанной папки. Исполняемые файлы программ копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию.

► *Чтобы настроить управление запуском программ на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. В рабочей области папки **Категории программ** создайте категории программ, запуском которых вы хотите управлять (см. раздел "Создание категорий программ" на стр. 388).
3. В папке **Управляемые устройства** на закладке **Политики** по ссылке **Новая политика Kaspersky Endpoint Security 11 для Windows** запустите мастер создания политики для программы Kaspersky Endpoint Security 11 для Windows и следуйте указаниям мастера.

   Если такая политика уже существует, этот шаг можно пропустить. Управление запуском программ в указанной категории можно настроить в параметрах этой политики. Созданная политика отображается в папке **Управляемые устройства** на закладке **Политики**.

4. В контекстном меню политики для программы Kaspersky Endpoint Security 11 для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики Kaspersky Endpoint Security 11 для Windows.

5. В окне свойств политики Kaspersky Endpoint Security 11 для Windows, в разделе **Контроль безопасности** → **Контроль программ** установите флажок **Контроль программ**.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля программ**.

7. В окне **Правило Контроля программ** в раскрывающемся списке **Категория** выберите категорию программ, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории программ.

   Для программ версий Kaspersky Endpoint Security для Windows 10 Service Pack 2 и выше категории, созданные по критерию MD5-хеша исполняемого файла, программы не отображаются.

   Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для программ версий ниже Kaspersky Endpoint Security для Windows 10 Service Pack 2. Это может привести к сбою программы.

   Подробные инструкции по настройке правил контроля приведены в онлайн-справке Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.1.0/ru-RU/127971.htm.

8. Нажмите на кнопку **ОК**.

Запуск программ на устройствах, входящих в указанную категорию, будет выполняться согласно созданному правилу. Созданное правило отображается в окне свойств политики Kaspersky Endpoint Security 11 для Windows в разделе **Контроль программ**.

Просмотр результатов статического анализа правил запуска исполняемых файлов

► *Чтобы просмотреть информацию о том, запуск каких исполняемых файлов запрещен пользователям, выполните следующие действия:*

1. В дереве консоли в папке **Управляемые устройства** выберите закладку **Политики**.
2. В контекстном меню политики для программы Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики программы.

3. В окне свойств политики выберите раздел **Контроль безопасности**, а затем подраздел **Контроль программ**.
4. Нажмите на кнопку **Статический анализ**.

   Откроется окно **Анализ списка прав доступа**. В левой части окна отображается список пользователей, основанный на данных Active Directory.

5. Выберите в списке пользователя.

   В правой части окна отобразятся категории программ, назначенные этому пользователю.

6. Чтобы просмотреть исполняемые файлы, запуск которых запрещен пользователю, в окне **Анализ списка прав доступа** нажмите на кнопку **Просмотреть файлы**.

   Откроется окно, в котором отображается список исполняемых файлов, запуск которых запрещен пользователю.

7. Чтобы просмотреть список исполняемых файлов, входящих в категорию, выберите категорию программ и нажмите на кнопку **Просмотреть файлы категории**.

   В открывшемся окне отображается список исполняемых файлов, входящих в категорию программ.

Просмотр реестра программ

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных программах из реестра Windows.

Получение информации об установленных программах поддерживается только для операционных систем Microsoft Windows.

► *Чтобы просмотреть реестр установленных на клиентских устройствах программ,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Реестр программ**.

В рабочей области папки **Реестр программ** отображается список программ, установленных на клиентских устройствах и Сервере администрирования.

Вы можете просмотреть подробную информацию о любой программе, выбрав в контекстном меню этой программы пункт **Свойства**. В окне свойств программы отображается общая информация о программе и информация об исполняемых файлах программы, а также список устройств, на которых установлена программа.

В контекстном меню любой программы вы можете:

- добавить эту программу в категорию программ;
- назначить тег программе;
- экспортировать список программ в файлы форматов CSV или TXT;
- просмотреть свойства программы, например, имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлена программа, список доступных обновлений программного обеспечения, список обнаруженных уязвимостей программного обеспечения.

Для просмотра программ, удовлетворяющих определенным критериям, вы можете воспользоваться полями фильтрации в рабочей области папки **Реестр программ**.

В окне свойств выбранного устройства (см. раздел "Параметры управляемого устройства" на стр. 617), вы можете просмотреть список программ, установленных на устройстве.

Генерация отчета об установленных программах

Вы также можете в рабочей области **Реестр программ** нажать на кнопку **Просмотреть отчет об установленных программах**, чтобы сгенерировать отчет, содержащий информацию об установленных программах, включая количество устройств, на которых установлена каждая программа. Этот отчет, который откроется на странице **Отчет об установленных программах** содержит информацию о программах "Лаборатории Касперского" и о программах сторонних производителей. Если вам нужна информация только о программах "Лаборатории Касперского", установленных на клиентских устройствах, в списке **Сводная информация** выберите "Лаборатория Касперского". Откроется окно **Отчет о версиях программ Лаборатории Касперского**.

Информация о программах "Лаборатории Касперского" и других производителей на устройствах, подключенных к подчиненным и виртуальным Серверам администрирования, также хранится в реестре программ главного Сервера администрирования. После добавления данных с подчиненных и виртуальных Серверов нажмите на кнопку **Просмотреть отчет об установленных программах** и на открывшейся странице **Отчет об установленных программах** вы можете просмотреть эту информацию.

► *Чтобы добавить информацию с подчиненных и виртуальных Серверов администрирования в отчет об установленных программах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. На закладке **Отчеты** выберите **Отчет об установленных программах**.
4. В контекстном меню отчета выберите пункт **Свойства**.

   Откроется окно **Свойства: Отчет об установленных программах**.
5. В разделе **Иерархия Серверов администрирования** установите флажок **Использовать данные с подчиненных и виртуальных Серверов администрирования**.
6. Нажмите на кнопку **ОК**.

В результате информация с подчиненных и виртуальных Серверов администрирования будет включена в отчет **Отчет о версиях программ "Лаборатории Касперского"**.

Создание групп лицензионных программ

► *Чтобы создать группу лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. По ссылке **Добавить группу лицензионных программ** запустите **Мастер добавления группы лицензионных программ**.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается группа лицензионных программ, которая отображается в папке **Учет сторонних лицензий**.

Управление ключами для групп лицензионных программ

► *Чтобы создать ключ для группы лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. В рабочей области папки **Учет сторонних лицензий** нажмите на кнопку **Управлять ключами лицензионных программ**

   Откроется окно **Управление ключами лицензионных программ**.
3. В окне **Управление ключами лицензионных программ** нажмите на кнопку **Добавить**.

   Откроется окно **Ключ**.
4. В окне **Ключ** укажите свойства ключа и ограничения, которые этот ключ накладывает на группу лицензионных программ.
   - **Название**. Название ключа.
   - **Комментарий**. Примечания к выбранному ключу.
   - **Ограничение**. Количество устройств, на которых может быть установлена программа, использующая этот ключ.
   - **Дата окончания**. Дата окончания срока действия ключа.

Созданные ключи отображаются в окне **Управление ключами лицензионных программ**.

► *Чтобы применить ключ к группе лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. В папке **Учет сторонних лицензий** выберите группу лицензионных программ, к которой вы хотите применить ключ.
3. В контекстном меню группы лицензионных программ выберите пункт **Свойства**.

Откроется окно свойств группы лицензионных программ.

4. В окне свойств группы лицензионных программ в разделе **Ключи** выберите вариант **Контролировать нарушение заданных лицензионных ограничений**.
5. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор ключа**.
6. В окне **Выбор ключа** выберите ключ, который вы хотите применить к группе лицензионных программ.
7. Нажмите на кнопку **ОК**.

Ограничения для группы лицензионных программ, указанные в ключе, будут распространены на выбранную группу лицензионных программ.

Изменение времени начала инвентаризации программного обеспечения

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Windows.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных программах из реестра Windows.

Чтобы сохранить ресурсы устройства, по умолчанию Агент администрирования начинает получать информацию об установленных программах через 10 минут после запуска службы Агента администрирования.

► *Чтобы изменить время начала инвентаризации программного обеспечения устройства после запуска службы Агента администрирования, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Агент администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
3. Для ключа KLINV_INV_COLLECTOR_START_DELAY_SEC установите нужное вам значение в секундах.

По умолчанию указано значение 600 секунд.

4. Перезапустите службу Агента администрирования.

В результате время начала инвентаризации программного обеспечения после запуска службы Агента администрирования изменится.

Инвентаризация исполняемых файлов

Инвентаризацию исполняемых файлов на клиентских устройствах можно выполнить с помощью задачи инвентаризации. В Kaspersky Endpoint Security 10 для Windows и в более поздних версиях реализована инвентаризация исполняемых файлов.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате работы мастера создается задача инвентаризации для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

Список исполняемых файлов, обнаруженных на устройствах в результате выполнения инвентаризации, отображается в рабочей области папки **Исполняемые файлы**.

При выполнении инвентаризации программа обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, а также HTML-файлы.

Просмотр информации об исполняемых файлах

► *Чтобы просмотреть список всех исполняемых файлов, обнаруженных на клиентских устройствах,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Исполняемые файлы**.

В рабочей области папки **Исполняемые файлы** отображается список исполняемых файлов, которые запускались на устройствах с момента установки операционной системы или были обнаружены в процессе работы задачи инвентаризации Kaspersky Endpoint Security для Windows.

Для просмотра данных об исполняемых файлах, удовлетворяющих определенным критериям, вы можете воспользоваться фильтрацией.

► *Чтобы просмотреть свойства исполняемого файла,*

в контекстном меню файла выберите пункт **Свойства**.

Откроется окно, содержащее информацию об исполняемом файле, а также список устройств, на которых присутствует исполняемый файл.

Уязвимости в программах

Папка **Уязвимости в программах**, входящая в состав папки **Управление программами**, содержит список уязвимостей в программах, которые обнаружил на клиентских устройствах установленный на них Агент администрирования. Агент администрирования выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях.

Функциональность анализа информации об уязвимостях в программах поддерживается только для операционных систем Microsoft Windows.

Открыв окно свойств выбранной программы в папке **Уязвимости в программах**, вы можете получить общую информацию об уязвимости, о программе, в которой она обнаружена, просмотреть список устройств, на которых обнаружена уязвимость, а также информацию о закрытии уязвимости.

Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (https://threats.kaspersky.com/ru/).

В этом разделе

Просмотр информации об уязвимостях в программах

► *Чтобы просмотреть список уязвимостей, обнаруженных на клиентских устройствах,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.

В рабочей области папки отображается список уязвимостей в программах на устройствах, которые

обнаружил Агент администрирования, установленный на них.

► *Чтобы получить информацию о выбранной уязвимости,*

в контекстном меню уязвимости выберите пункт **Свойства**.

Откроется окно свойств уязвимости, в котором отображается следующая информация:

- программа, в которой обнаружена уязвимость;
- список устройств, на которых обнаружена уязвимость;
- информация о закрытии уязвимости.

► *Чтобы просмотреть отчет обо всех обнаруженных уязвимостях,*

в папке **Уязвимости в программах** воспользуйтесь ссылкой **Просмотреть отчет об уязвимостях в программах**.

Будет создан отчет об уязвимостях в программах, установленных на устройствах. Отчет можно просмотреть в узле с именем нужного вам Сервера администрирования на закладке **Отчеты**.

Функция получения информации об уязвимостях в программах поддерживается только для операционных систем Microsoft Windows.

Поиск уязвимостей в программах

Если вы выполнили настройку программы с помощью мастера первоначальной настройки, задача поиска уязвимостей создается автоматически. Просмотреть задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

► *Чтобы создать задачу поиска уязвимостей в программах, установленных на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами**, выберите вложенную папку **Уязвимости в программах**.
2. В рабочей области папки нажмите на кнопку **Дополнительные действия** → **Настроить поиск уязвимостей**.

   Если задача для поиска уязвимостей уже существует, она отображается на закладке **Задачи** в папке **Управляемые устройства**, с существующими выбранными задачами. В противном случае запускается мастер создания задачи поиска уязвимостей и требуемых обновлений. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В окне **Выбор типа задачи** выберите **Поиск уязвимостей и требуемых обновлений**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:

- **Использовать данные служб Windows Server Update Services**

При поиске уязвимостей и программ, для которых требуются обновления, Kaspersky Security Center использует информацию о применимых обновлениях Microsoft Windows из источника обновлений Microsoft.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Подключаться к серверу обновлений для получения новых данных**

Если этот параметр включен, Kaspersky Security Center подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Kaspersky Security Center использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Поэтому рекомендуется выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах обновлений Windows.

По умолчанию параметр включен.

- **Использовать список программ, предоставленный "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине

значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств.Утилита удаленной диагностики Kaspersky Security Center" на стр. 608), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

Максимальный объем дискового пространства в мегабайтах (МБ), который может быть занят файлами расширенной диагностики.

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный

день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании

задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача Поиск уязвимостей и требуемых обновлений, которая отображается в списке задач, в папке **Управляемые устройства**, на закладке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Когда задача поиска уязвимостей и требуемых обновлений завершена, Сервер администрирования отображает список уязвимостей, обнаруженных в программах, установленных на устройстве; также Сервер отображает все обновления программного обеспечения, необходимые для исправления обнаруженных уязвимостей.

Сервер администрирования не отображает список необходимых обновлений программного обеспечения при последовательном запуске двух задач: задачи синхронизации обновлений Windows Update, для которой отключен параметр **Загружать файлы экспресс-установки**, и затем задачи поиска уязвимостей и требуемых обновлений. Чтобы просмотреть список необходимых обновлений программного обеспечения, необходимо снова запустить задачу поиска уязвимостей и требуемых обновлений.

Агент администрирования получает информацию о любых доступных обновлениях Windows и других программ Microsoft от Центра обновления Windows или от Сервера администрирования, если Сервер

администрирования выполняет роль WSUS-сервера. Информация передается при запуске программ (если это предусмотрено политикой) и при каждом запуске задачи поиска уязвимостей и требуемых обновлений на клиентских устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе **Управление Сервером** (**https://support.kaspersky.com/14758**).

Закрытие уязвимостей в программах

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача **Установка требуемых обновлений и закрытие уязвимостей** создается автоматически. Задача отображается в папке **Управляемые устройства** на закладке **Задачи**.

В противном случае вы можете выполнить одно из следующих действий:

- Создайте задачу для закрытия уязвимостей с помощью установки доступных обновлений.
- Добавьте правило для закрытия уязвимостей в существующую задачу закрытия уязвимостей.

Закрытие уязвимостей с помощью задачи закрытия уязвимостей

Выполните одно из следующих действий:

- Создайте задачу закрытия нескольких уязвимостей, соответствующих определенным правилам.
- Выберите уязвимость и создайте задачу для ее закрытия и для закрытия аналогичных уязвимостей.

► *Чтобы закрыть уязвимости, которые соответствуют определенным правилам, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Задачи**.
3. По кнопке **Создать задачу** запустите мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне **Выбор типа задачи** мастера создания задачи выберите **Установка требуемых обновлений и закрытие уязвимостей**.
5. В окне мастера **Параметры**, укажите следующие параметры задачи:
    - **Укажите правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений(см. стр. 423).

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением

устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии программы при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая**

Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать

трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств.Утилита удаленной диагностики Kaspersky Security Center" на стр. 608), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

Максимальный объем дискового пространства в мегабайтах (МБ), который может быть занят файлами расширенной диагностики.

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

В месяцах, у которых нет указанного дня, задача выполняется в последний день.

По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы

можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

► *Чтобы закрыть требуемую уязвимость и аналогичные ей, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную

папку **Уязвимости в программах**.

2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

   > Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

   Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

   - **Искать задачи, закрывающие выбранную уязвимость**

Если этот параметр включен, мастер закрытия уязвимостей выполняет поиск существующих задач для закрытия выбранной уязвимости.

Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимостей предлагает создать правило или задачу для закрытия уязвимости.

По умолчанию параметр включен.

- **Одобрить обновления, закрывающие выбранную уязвимость**

Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Новая задача закрытия уязвимости**.
2. Выберите тип правила, закрывающего уязвимость, чтобы добавить его в существующую задачу и нажмите на кнопку **Готово**.
3. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих параметров:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или сканировать устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

   - **Назначить задачу группе администрирования**

     В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

В месяцах, у которых нет указанного дня, задача выполняется в последний день.

По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы

можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Закрытие уязвимости с помощью добавления правила в существующую задачу закрытия уязвимостей

► *Чтобы закрыть уязвимость с помощью добавления правила в существующую задачу закрытия*

уязвимостей, выполните следующие действия:

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.
2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

   > Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

   Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

   - **Искать задачи, закрывающие выбранную уязвимость**

Если этот параметр включен, мастер закрытия уязвимостей выполняет поиск существующих задач для закрытия выбранной уязвимости.

Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимостей предлагает создать правило или задачу для закрытия уязвимости.

По умолчанию параметр включен.

- **Одобрить обновления, закрывающие выбранную уязвимость**

Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Добавить правило закрытия уязвимости в существующую задачу**.
2. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.
3. Выберите тип правила, чтобы добавить его в выбранную задачу, и нажмите на кнопку **Готово**.
4. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая

последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

Новое правило для закрытия уязвимости добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Правила установки обновлений

Для закрытия уязвимостей в программах (см. стр. 409), необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, создаете ли вы правило для обновлений программ Microsoft, программ сторонних производителей (программ, производимых поставщиками программного обеспечения, кроме "Лаборатории Касперского" и Microsoft) или всех программ. При создании правила для программ Microsoft или программ сторонних производителей вы можете выбрать программы и версии программ, для которых вы хотите установить обновления. При создании правила для всех программ вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

► Чтобы создать правило для обновления программ, выполните следующие действия:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. В окне **Тип правила** выберите **Правило для всех обновлений**.
3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:
   - Набор обновлений для установки

     Выберите обновления из раскрывающегося списка, которые должны быть установлены на клиентском устройстве:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*. Выбрано по умолчанию.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.
   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного

обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Обновления** выберите обновления для установки:

   - **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные программы или чтобы обновить только требуемые программы.

   - **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

1. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрывать только уязвимости из списка**

Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных программах или чтобы закрыть уязвимости только в требуемых программах.

1. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

► Чтобы создать правило обновления программ Microsoft, выполните следующие действия:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. В окне **Тип правила** выберите **Правило для обновлений Windows Update**.
3. В окне **Общие условия** настройте следующие параметры:
   - Набор обновлений для установки

     Выберите обновления из раскрывающегося списка, которые должны быть установлены на клиентском устройстве:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*. Выбрано по умолчанию.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.
   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не

закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
3. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

► Чтобы создать правило для обновления программ сторонних производителей, выполните следующие действия:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. В окне **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления из раскрывающегося списка, которые должны быть установлены на клиентском устройстве:

     - **Устанавливать только утвержденные обновления**. В этом случае

устанавливаются только одобренные обновления.

- **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*. Выбрано по умолчанию.
- **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

См. также:

Одобрение и отклонение обновлений программного обеспечения 430

Обновления программного обеспечения

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения, установленного на клиентских устройствах, и закрывать уязвимости в программах Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи поиска обновлений и загружает

обновления в хранилище обновлений. После завершения поиска обновлений программа предоставляет администратору информацию о доступных обновлениях и об уязвимостях в программах, которые можно закрыть с помощью этих обновлений.

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Для использования Сервера администрирования в роли сервера Windows Update необходимо настроить синхронизацию обновлений с центром обновлений Windows. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

Управлять обновлениями программного обеспечения можно также с помощью политики Агента администрирования. Для этого необходимо создать политику Агента администрирования и настроить параметры обновлений программного обеспечения в соответствующих окнах мастера создания политики.

Администратор может просматривать список доступных обновлений в папке **Обновления программного обеспечения**, входящей в состав папки **Управление программами**. Эта папка содержит список полученных Сервером администрирования обновлений программ Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. После просмотра информации о доступных обновлениях администратор может выполнить установку обновлений на устройства.

Обновление некоторых программ Kaspersky Security Center выполняет путем удаления предыдущей версии программы и установки новой версии.

Перед установкой обновлений на все устройства можно выполнить проверочную установку, чтобы убедиться, что установленные обновления не вызовут сбоев в работе программ на устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе Управление Сервером (https://support.kaspersky.ru/14758).

В этом разделе

Просмотр информации о доступных обновлениях

► *Чтобы просмотреть список доступных обновлений для программ, установленных на клиентских устройствах,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.

В рабочей области папки вы можете просматривать список имеющихся обновлений для программ, установленных на устройствах.

► *Чтобы просмотреть свойства обновления,*

в рабочей области папки **Обновления программного обеспечения** в контекстном меню обновления выберите пункт **Свойства**.

В окне свойств обновления для просмотра доступна следующая информация:

- список клиентских устройств, для которых применимо обновление;
- список общесистемных компонентов (пререквизитов), которые должны быть установлены перед обновлением (любым);
- уязвимости в программах, которые закрывают это обновление.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

► *Чтобы подтвердить или отменить одно или несколько обновлений, выполните следующие действия:*

1. В дереве консоли выберите узел **Дополнительно → Управление программами → Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** перейдите по ссылке **Обновить** вверху справа и дождитесь загрузки списка обновлений. Отобразится список обновлений.
3. Выберите обновления, которые требуется подтвердить или отклонить.

   Блок работы с выбранным объектом отображается в правой части рабочей области.
4. В раскрывающемся списке **Одобрение обновления** выберите **Одобрено**, чтобы подтвердить выбранные обновления, или **Отклонено**, чтобы отменить выбранные обновления.

   По умолчанию установлено значение **Не определено**.

Обновления, для которых установлен статус **Одобрено**, помещаются в очередь на установку.

Обновления, для которых установлен статус **Отклонено**, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для программ "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус **Отклонено**, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.
Если обновления для программ "Лаборатории Касперского" не могут быть удалены, это отображается в окне свойств обновления: в разделе **Общие** и в разделе **Требования при установке**.
Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

Синхронизация обновлений Windows Update с Сервером администрирования

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Использовать Сервер администрирования в роли WSUS-сервера**, задача синхронизации обновлений Windows Update создается автоматически. Запустить задачу можно в папке **Задачи**. Функция

обновления программного обеспечения Microsoft доступна только после успешного завершения задачи **Синхронизация обновлений Windows Update**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы создать задачу синхронизации обновлений Windows Update с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить синхронизацию обновлений Windows Update**.

   В результате работы мастера создается задача **Синхронизация обновлений Windows Update**, которая отображается в папке **Задачи**.

   Запустится мастер создания задачи получения данных из центра обновлений Windows. Следуйте далее указаниям мастера.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Microsoft периодически удаляет со своих серверов устаревшие обновления так, что число актуальных обновлений составляет от 200 000 до 300 000. В Kaspersky Security Center 10 версии Service Pack 2 Maintenance Release 1 и ниже сохранялись все обновления, устаревшие обновления не удалялись. Это приводило к постоянному росту размера базы данных. Для уменьшения используемого дискового пространства и размера базы данных в Kaspersky Security Center 10 Service Pack 3 реализовано удаление устаревших обновлений, которые отсутствуют на серверах обновлений Microsoft.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, программа получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание базы данных** (см. раздел "**Обслуживание базы данных Сервера администрирования**" на стр. 849) можно удалить такие устаревшие записи из базы данных и

соответствующих им файлов.

В этом разделе

Шаг 1. Параметры

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, снимите флажок **Загружать файлы экспресс-установки**.

Если флажок установлен, в процессе выполнения задачи загружаются файлы экспресс-установки.

По умолчанию флажок снят.

Шаг 2. Программы

В этом разделе можно выбрать программы, для которых будут загружаться обновления.

Если установлен флажок **Все программы**, то обновления будут загружаться для всех имеющихся программ, а также для тех программ, которые могут быть выпущены в будущем.

По умолчанию флажок **Все программы** установлен.

Шаг 3. Категории обновлений

В этом разделе можно выбрать категории обновлений, которые будут загружаться на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий

обновлений, а также для тех категорий, которые могут появиться в будущем.

По умолчанию флажок **Все категории** установлен.

Шаг 4. Языки локализации обновлений

В этом окне можно выбрать языки локализации обновлений, которые будут загружаться на Сервер администрирования. Выберите один из следующих вариантов загрузки языков локализации обновлений:

- **Загружать все языки, включая новые**

  Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

  Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

Шаг 5. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию.**

  Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

  По умолчанию выбран этот вариант.

- **Задать учетную запись:**

  Поля **Учетная запись** и **Пароль** становятся доступными для изменения. Заполните эти поля, чтобы указать данные учетной записи, которая имеет необходимые права для выполнения.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль.**

    Пароль учетной записи, от имени которой будет запускаться задача.

Шаг 6. Настройка расписания запуска задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Каждый N час**

Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее

системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

Шаг 7. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).По умолчанию задано значение *Синхронизация обновлений Windows Update*.

Шаг 8. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Созданная задача синхронизации обновлений Windows Update отобразится в списке задач в папке **Задачи** дерева консоли.

Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства

Вы можете настроить автоматическое обновление баз и модулей программы Kaspersky Endpoint Security на клиентских устройствах.

► *Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security на устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Создайте задачу с типом **Обновление** одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать → Задачу**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Обновление**.
4. Следуйте дальнейшим шагам мастера.

   В результате работы мастера создается задача обновления для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.
5. В рабочей области папки **Задачи** выберите созданную задачу обновления.
6. В контекстном меню задачи выберите пункт **Поиск**.
7. В открывшемся окне свойств задачи выберите раздел **Свойства**.

   В разделе **Свойства** можно настроить параметры задачи обновления в локальном и мобильном режимах:
   - **Параметры обновления в локальном режиме**: между устройством и Сервером администрирования установлена связь.
   - **Параметры обновления в мобильном режиме**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).
8. По кнопке **Параметры** выберите источник обновлений.
9. Установите флажок **Загружать обновления модулей программы**, чтобы одновременно с базами программы загружать и устанавливать обновления модулей программы.

   Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей программы и во время выполнения задачи обновления включает обновления модулей программы в пакет обновлений. Настройте применение модулей обновлений:
   - **Устанавливать критические и одобренные обновления**. При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей программы – после одобрения их установки администратором.

- **Устанавливать только утвержденные обновления**. При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то программа устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

10. Установите флажок **Копировать обновления в папку**, чтобы программа сохраняла загруженные обновления в папку, указанную по кнопке **Обзор**.
11. Нажмите на кнопку **ОК**.

При выполнении задачи **Обновление** программа отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых программ.

Офлайн-модель получения обновлений

Агент администрирования на управляемых устройствах не всегда может подключиться к Серверу администрирования для получения обновлений. Например, Агент администрирования может быть установлен на ноутбук, который иногда не подключен к интернету и локальной сети. Также администратор может ограничить время подключения устройств к сети. В таких случаях устройства с установленным Агентом администрирования не смогут получить обновления от Сервера администрирования в соответствии с расписанием. Если настроено обновление управляемых программ (например, Kaspersky Endpoint Security) с помощью Агента администрирования, для обновления требуется соединение с Сервером администрирования. Когда соединение между Агентом администрирования и Сервером администрирования отсутствует, обновление невозможно. Соединение Агента администрирования с Сервером может быть настроено так, чтобы Агент подключался к Серверу только в определенные периоды времени. В худшем случае, если настроенные периоды подключения "пересекаются" с периодами, когда связь отсутствует, базы никогда не будут обновлены. Также возможны ситуации, когда много управляемых программ одновременно обращаются к Серверу администрирования за обновлениями. В этом случае Сервер администрирования может перестать отвечать на запросы (как во время DDoS-атаки).

Во избежание описанных проблем в Kaspersky Security Center реализована офлайн-модель получения обновления баз и модулей управляемых программ. Эта модель обеспечивает надежность механизма распространения обновлений вне зависимости от временных проблем недоступности каналов связи сервера администрирования, а также снижает нагрузку на Сервер администрирования. Эта модель также снижает нагрузку на Сервер администрирования.

Как работает офлайн-модель получения обновлений

Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые

потребуются для управляемых программ. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для программ на клиентских устройствах, но подключение не требуется для обновления.

Чтобы распределить нагрузку на Сервер администрирования, Агент администрирования на устройстве подключается к Серверу и загружает обновления случайным образом в течение интервала времени, определенного Сервером. Интервал времени зависит от количества устройств с установленным Агентом администрирования, которые загружают обновления, и от размера обновлений. Для снижения нагрузки на Сервер администрирования вы можете использовать Агент администрирования в качестве точки распространения.

Если офлайн-модель получения обновлений отключена, обновления распространяются в соответствии с расписанием задачи загрузки обновлений в хранилище.

По умолчанию офлайн-модель получения обновлений включена.

Офлайн-модель получения обновлений используется только для тех управляемых устройств, на которых задача получения обновлений управляемыми программами имеет расписание **При загрузке обновлений в хранилище**. Для остальных управляемых устройств используется традиционная система получения обновлений с Сервера администрирования в реальном времени.

Рекомендуется выключить офлайн-модель получения обновлений через настройки политик Агента администрирования соответствующих групп администрирования, если в управляемых программах настроено получение обновлений не с Сервера администрирования, а с серверов "Лаборатории Касперского" либо из сетевой папки и при этом задача получения обновлений имеет расписание **При загрузке обновлений в хранилище**.

См. также:

Включение и выключение офлайн-модели получения обновлений.....440

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Технической поддержки "Лаборатории Касперского" могут рекомендовать вам снять флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для программ "Лаборатории Касперского" настроена.

► *Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

   По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

См. также:

Офлайн-модель получения обновлений 438

Установка обновлений на устройства вручную

Если в окне **Параметры управления обновлениями** мастера первоначальной настройки вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача Установка требуемых обновлений и закрытие уязвимостей создается автоматически. Остановить или запустить задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

Если в мастере первоначальной настройки вы выбрали вариант **Искать требующиеся для установки обновления**, вы можете установить обновления программного обеспечения на клиентские устройства с помощью задачи **Установка требуемых обновлений и закрытие уязвимостей**.

Выполните одно из следующих действий:

- Создайте задачу для установки обновлений.
- Добавьте правило для установки обновления в существующую задачу установки обновлений.
- В параметрах существующей задачи установки обновлений настройте тестовую установку обновлений.

Установка обновлений с помощью создания задачи установки обновлений

Выполните одно из следующих действий:

- Создайте задачу для установки требуемых обновлений.
- Выберите обновление и создайте задачу для его установки и для установки аналогичных обновлений.

► *Чтобы установить требуемые обновления, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки выберите обновление, которое вы хотите установить.
3. Выполните одно из следующих действий:
   - В контекстном меню выбранного обновления выберите пункт **Установить обновление** → **Создать задачу**.
   - Перейдите по ссылке **Установить обновление (создать задачу)** в блоке работы с выбранным обновлением.
4. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:
   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

Задача выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится

видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), перед

установкой обновления в свойствах задачи Установка требуемых обновлений и закрытие уязвимостей. Когда параметр включен, все требуемые общесистемные компоненты устанавливаются перед обновлением. Список этих компонентов можно посмотреть в свойствах обновления.

В свойствах задачи Установка требуемых обновлений и закрытие уязвимостей вы можете разрешить установку обновлений, которые обновляют программу до новой версии.

Если в параметрах задачи настроены правила установки обновлений сторонних производителей, Сервер администрирования загружает с сайта производителей требуемые обновления. Обновления сохраняются в хранилище Сервера администрирования и далее распространяются и устанавливаются на устройства, где они применимы.

Если в параметрах задачи настроены правила установки обновлений Microsoft и Сервер администрирования используется в качестве WSUS-сервера, Сервер администрирования загружает необходимые обновления в хранилище и далее распространяет на управляемые устройства. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы установить требуемое обновление и аналогичные обновления, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   > Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне **Поиск существующих задач установки обновления** задайте следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Создать задачу установки обновления**.

2. Выберите тип правила установки, чтобы добавить его в новую задачу и нажмите на кнопку **Готово**.

3. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Спросить у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

     - **Повторять запрос каждые (мин)**

Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих параметров:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или сканировать устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете

выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

После установки новой версии программы может быть нарушена работа других программ, установленных на устройствах и зависящих от работы обновляемой программы.

Установка обновления с помощью добавления правила в существующую задачу

► *Чтобы установить обновление с помощью добавления правила в существующую задачу, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Для продолжения работы мастера нажмите на кнопку **Далее**.
4. В окне **Поиск существующих задач установки обновления** задайте следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае, нажмите на кнопку **Добавить правило установки обновления**.

2. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

3. Выберите тип правила, которое будет добавлено в выбранную задачу, и нажмите на кнопку **Готово**.

4. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

Новое правило для установки обновления добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Настройка проверочной установки обновлений

► *Чтобы настроить проверочную установку обновлений, выполните следующие действия:*

1. В дереве консоли в папке **Управляемые устройства** на закладке **Задачи** выберите задачу **Установка требуемых обновлений и закрытие уязвимостей**.

2. В контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно свойств задачи **Установка требуемых обновлений и закрытие уязвимостей**.

3. В окне свойств задачи в разделе **Проверочная установка** выберите один из доступных вариантов проверочной установки:

   - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.

   - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

   - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.

- **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

4. После выбора любого параметра, кроме **Не проверять**, в поле **Время для принятия решения о продолжении установки (ч.)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

Настройка обновлений Windows в политике Агента администрирования

► *Чтобы настроить обновления Windows в политике Агента администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Политики**.
3. Выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики Агента администрирования выберите раздел **Обновления и уязвимости в программах**.
6. Установите флажок **Использовать Сервер администрирования в роли WSUS-сервера**, чтобы загружать обновления Windows на Сервер администрирования и затем распространять их на клиентские устройства средствами Агента администрирования.

   Если флажок снят, обновления Windows не загружаются на Сервер администрирования. В этом случае клиентские устройства получают обновления Windows напрямую с серверов Microsoft.
7. Выберите набор обновлений, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

   > Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, новый параметр, который вы выбрали **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

   Выберите параметр из раскрывающегося списка:

   - **Устанавливать все применимые обновления Центра обновления Windows**

     Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

     Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

1. Выберите режим поиска обновлений Windows Update:

- **Активна.**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при

последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен**

  Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

2. Установите флажок **Проверять исполняемые файлы на наличие уязвимостей при запуске**, чтобы при запуске исполняемых файлов выполнять их проверку на наличие уязвимостей.
3. Нажмите на кнопку **Применить**.

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center

По умолчанию автоматически устанавливаются загруженные обновления и патчи для следующих компонентов программы (начиная с версии Kaspersky Security Center 10 Service Pack 2):

- Агент администрирования для Windows;
- Консоль администрирования;
- Сервер мобильных устройств Exchange ActiveSync;
- Сервер iOS MDM.

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center доступна только для устройств под управлением Windows. Вы можете выключить автоматическую установку обновлений и патчей для этих компонентов. В этом случае загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

См. также:

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center 458

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство, выполните следующие действия:*

1. Запустите локальную установку Агента администрирования на устройство (см. раздел "Локальная установка Агента администрирования" на стр. 138).
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета, выполните следующие действия:*

1. В дереве консоли выберите папку **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню пакета **Агент администрирования Kaspersky Security Center <номер версии>** выберите пункт **Свойства**.
3. В свойствах инсталляционного пакета в разделе **Параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

► *Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить или выключить автоматическую установку обновлений и патчей.

2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**, чтобы соответственно включить или выключить автоматическую установку.
7. Установите замок при этом флажке.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

См. также:

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center 457

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

- Индикаторы

  В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов.

- Статистика

  Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей.

- Отчеты

  Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

- События

  Выборки событий предназначены для просмотра на экране именованных наборов событий, которые хранятся в базе данных Сервера администрирования. Эти выборки событий сгруппированы по уровням важности (**Критические события**, **Отказ функционирования**, **Предупреждения** и **Информационные сообщения**), по времени (**Недавние события**) и по типу (**Пользовательские запросы** и **События аудита**.

В этом разделе

Цветовые индикаторы в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов. Индикаторы отображаются в рабочей области

узла **Сервер администрирования** на закладке **Мониторинг**. На закладке имеется шесть информационных блоков с цветовыми индикаторами. Цветной индикатор – это цветная вертикальная полоса на левой стороне панели. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

Таблица 43. Области ответственности цветовых индикаторов в Консоли администрирования

Название панели	Область ответственности цветового индикатора
Развертывание	Установка Агента администрирования и программ безопасности на устройства сети организации.
Структура управления	Структура групп администрирования. Сканирование сети. Правила перемещения устройств.
Настройка защиты	Функции программы безопасности: состояние защиты, поиск вирусов.
Обновление	Обновления и патчи.
Мониторинг	Состояние защиты
Сервер администрирования	Функции и свойства Сервера администрирования.

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

Таблица 44. Цветовые кодировки индикаторов

Состояние	Цвет индикатора	Значение цвета индикатора
Информационное	Зеленый	Вмешательство администратора не требуется.
Предупреждение	Желтый	Требуется вмешательство администратора.
Предельный.	Красный	Имеются серьезные проблемы. Требуется вмешательство администратора для их решения.
Информационное	Голубой	Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств.
Информационное	Серый	Информация о событиях недоступна или еще не получена.

Цель администратора поддерживать индикаторы в состоянии "зеленый" на всех информационных панелях закладки **Мониторинг**.

Работа с отчетами, статистикой и уведомлениями

В этом разделе представлена информация о работе с отчетами, статистикой и выборками событий и устройств в Kaspersky Security Center, а также о настройке параметров уведомлений Сервера администрирования.

В этом разделе

Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Вы можете создавать отчеты для следующих объектов:

- для выборок устройств, созданных по определенным параметрам;
- для групп администрирования;
- для наборов устройств из разных групп администрирования;
- для всех устройств в сети (в отчете о развертывании).

В программе есть набор стандартных шаблонов отчетов. Предусмотрена также возможность создавать пользовательские шаблоны отчетов. Отчеты отображаются в главном окне программы, в папке дерева консоли **Сервер администрирования**.

В этом разделе

Создание шаблона отчета

► *Чтобы создать шаблон отчета, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   В результате запустится мастер создания шаблона отчета. Следуйте далее указаниям мастера.

После окончания работы мастера сформированный шаблон отчета будет добавлен в состав выбранной папки **Сервер администрирования** дерева консоли. Этот шаблон можно использовать для создания и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

► *Чтобы просмотреть и изменить свойства шаблона отчета, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.

   Также вы можете сначала создать отчет, а затем нажать на кнопку **Открыть свойства шаблона отчета** или на кнопку **Настроить графы отчета**.
5. В открывшемся окне вы можете изменить свойства шаблона отчета. Свойства каждого отчета могут содержать только некоторые из разделов, описанных ниже.
   - Раздел **Общие**
     - Название шаблона отчета

- **Максимальное число отображаемых записей**

Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Графы** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

По умолчанию параметр включен. По умолчанию указано значение 1000.

- **Версия для печати**

Отчет оптимизирован для печати: добавлены пробелы, между некоторыми значениями для лучшей визуальной доступности.

По умолчанию параметр включен.

- Раздел **Поля отчета**

  Выберите поля, которые будут отображаться в отчете и порядок этих полей. Также настройте, должна ли информация в отчете сортироваться и фильтроваться по каждому из полей.

- Раздел **Период**

  Измените отчетный период. Доступные значения:

  - между двумя указанными датами;
  - от указанной даты до даты создания отчета;
  - от даты создания отчета минус указанное количество дней до даты создания отчета.

- Разделы **Группа**, **Выборка устройств**, или **Устройства**

  Измените набор клиентских устройств, для которых создается отчет. В зависимости от параметров, указанных при создании шаблона, может присутствовать только один из этих разделов.

- Раздел **Параметры**

  Измените параметры отчета. Набор параметров зависит от конкретного отчета.

- Раздел **Безопасность**
  - **Наследовать параметры Сервера администрирования или родительской группы**

    Если этот параметр включен, параметры отчета наследуются с Сервера администрирования.

    Если этот параметр выключен, вы можете настроить параметры отчета. Вы можете назначить роль пользователю или группе пользователей (см. раздел "Назначение роли пользователю или группе пользователей" на стр. 647) или назначить права пользователю или группе пользователей (см. раздел "Назначение прав пользователям и группам пользователей" на стр. 648), применительно к отчету.

    По умолчанию параметр включен.

Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. 556).

- Раздел **Иерархия Серверов администрирования**
  - **Использовать данные с подчиненных и виртуальных Серверов администрирования**

Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

По умолчанию параметр включен.

- **До уровня вложенности**

Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

Включение этой опции позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

Подчиненные Серверы администрирования через заданные интервалы времени (указанные в часах) передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Если установлено значение 0, данные передаются только во время генерации отчета.

По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

По умолчанию параметр выключен.

Создание и просмотр отчета

► *Чтобы сформировать и просмотреть отчет, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов двойным нажатием клавиши мыши.

   Отобразится выбранный шаблон отчета.

В отчете отображаются следующие данные:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для

какой группы устройств создан отчет;

- графическая диаграмма с наиболее характерными данными отчета;
- сводная таблица с вычисляемыми показателями отчета;
- таблица с детальными данными отчета.

Сохранение отчета

► *Чтобы сохранить сформированный отчет, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.

В результате запустится мастер сохранения отчета. Следуйте далее указаниям мастера.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

Создание задачи рассылки отчета

Отчеты можно рассылать по электронной почте. Рассылка отчетов в Kaspersky Security Center осуществляется с помощью задачи рассылки отчета.

► *Чтобы создать задачу рассылки одного отчета, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Рассылка отчетов**.

В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте далее указаниям мастера.

► *Чтобы создать задачу рассылки нескольких отчетов, выполните следующие действия:*

1. В дереве консоли в узле с именем нужного вам Сервера администрирования выберите папку **Задачи**.
2. В рабочей области папки **Категории программ** нажмите на кнопку **Создать категорию**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 213).

В этом разделе

Шаг 1. Выбор типа задачи

В окне **Выбор типа задачи** в списке задач выберите тип задачи **Рассылка отчета**.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 2. Выбор типа отчета

В окне **Выбор типа отчета** в списке шаблонов для создания задачи выберите тип отчета.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 3. Действия с отчетом

В окне **Действия с отчетами** настройте следующие параметры:

- **Посылать отчеты по электронной почте**

  Если флажок установлен, программа отправляет сформированные отчеты по электронной почте.

  Параметры отправки отчета по электронной почте можно настроить по ссылке **Параметры уведомления по электронной почте**. Ссылка доступна, когда флажок установлен.

  Если флажок снят, программа сохраняет отчеты в указанной папке для хранения отчетов.

  По умолчанию флажок снят.

- **Сохранять отчеты в папке**

  Если флажок установлен, программа сохраняет отчеты в папке, указанной в поле под флажком. Чтобы сохранять отчеты в папке общего доступа, укажите UNC-путь к этой папке. В таком случае в окне **Выбор учетной записи для запуска задачи** необходимо задать учетную запись и пароль пользователя для доступа к этой папке.

  Если флажок снят, программа не сохраняет отчеты в папке, а отправляет их по электронной почте.

  По умолчанию флажок снят.

- **Замещать предыдущие отчеты того же типа**

  Если флажок установлен, при каждом запуске задачи новый файл отчета замещает в папке для хранения отчетов файл, сохраненный при предыдущем запуске задачи.

  Если флажок снят, файлы отчетов не перезаписываются. При каждом запуске задачи в папке сохраняется отдельный файл отчета.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

  По умолчанию флажок снят.

- **Задать учетную запись для доступа к папке общего доступа**

  Если флажок установлен, можно указать учетную запись, от имени которой отчет записывается в папку. Если в окне **Действия с отчетом** в качестве параметра **Сохранять отчет в папке** указан UNC-путь к папке общего доступа, необходимо указать учетную запись и пароль для доступа к этой папке.

  Если флажок снят, отчет записывается в папку от имени учетной записи Сервера администрирования.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

  По умолчанию флажок снят.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 4. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию.**

  Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

  По умолчанию выбран этот вариант.

- **Задать учетную запись:**

  Поля **Учетная запись** и **Пароль** становятся доступными для изменения. Заполните эти поля, чтобы указать данные учетной записи, которая имеет необходимые права

для выполнения.

- **Учетная запись**

  Учетная запись, от имени которой будет запускаться задача.

- **Пароль.**

  Пароль учетной записи, от имени которой будет запускаться задача.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 5. Настройка расписания задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени,

фактическое время запуска задачи не изменяется.

Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее

завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

Шаг 6. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 7. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Работа со статистической информацией

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей. Статистическая информация отображается в рабочей области узла **Сервер администрирования** на закладке **Статистика**. Эта закладка также содержит несколько закладок второго уровня (страниц). На каждой странице отображаются информационные панели со статистической информацией, а также ссылки на корпоративные новости и другие материалы "Лаборатории Касперского". Статистическая информация представлена на информационных панелях в виде круговых или столбчатых диаграмм или таблиц. Данные на информационных панелях обновляются в процессе работы программы и отражают текущее состояние программы безопасности.

Можно изменить набор закладок второго уровня, содержащихся на закладке **Статистика**, набор информационных панелей на каждой странице с закладками, а также способ представления данных на информационных панелях.

► *Чтобы добавить новую закладку второго уровня с информационными панелями на закладке **Статистика**, выполните следующие действия:*

1. Нажмите на кнопку **Настроить вид** в правом верхнем углу закладки **Статистика**.

   В результате откроется окно свойств статистики. В окне содержится список страниц с закладками, которые содержатся на закладке **Статистика** в настоящее время. В окне можно изменять порядок отображения страниц на закладке, добавлять и удалять страницы, переходить к настройке свойств страниц по кнопке **Свойства**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно свойств новой страницы.

3. Настройте новую страницу:

   - В разделе **Общие** укажите название страницы.

- В разделе **Информационные панели** по кнопке **Добавить** добавьте информационные панели, которые должны отображаться на странице.

  По кнопке **Свойства** в разделе **Информационные панели** можно настраивать свойства добавленных информационных панелей: название, тип и вид диаграммы на панели, данные, по которым строится диаграмма.

4. Нажмите на кнопку **ОК**.

Добавленная страница с закладками с информационными панелями отобразится на закладке **Статистика**. Нажав на значок **Параметры** ( ) можно сразу перейти к настройке страницы или выбранной информационной панели на странице.

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений.

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. раздел "Уведомление о событиях с помощью исполняемого файла" на стр. 234).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   В результате откроется окно **Свойства: События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

   - **Электронная почта**

На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. В качестве адреса можно

использовать IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры уведомлений (например, указать тему сообщения).

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильность настройки сообщений: программа отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

  На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

  В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

  В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. В качестве адреса можно использовать IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

  В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

  Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры уведомлений (например, указать тему сообщения).

  В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по

нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

  По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   > Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

   Программа отправляет тестовое уведомление указанному получателю.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. раздел "Общие параметры политик" на стр. 623) или параметров программы (см. раздел "Выбор событий для программы" на стр. 751).

См. также:

Обработка и хранение событий на Сервере администрирования.....557

Создание сертификата для SMTP-сервера

Сертификат для SMTP-сервера необходим для идентификации и верификации почтового сервера, к которому производится подключение. Сертификат используется для защиты пересылаемых писем от перехвата, например, в процессе передачи писем от почтового клиента к серверу и обратно.

► *Чтобы создать сертификат для SMTP-сервера, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно свойств событий.
4. На закладке **Электронная почта** по ссылке **Параметры** откройте окно **Параметры**.
5. В окне **Параметры** по ссылке **Задать сертификат** откройте окно **Сертификат для подписи**.
6. В окне **Сертификат для подписи** нажмите на кнопку **Задать**.

   В результате откроется окно **Сертификат**.
7. В раскрывающемся списке **Тип сертификата** выберите открытый или закрытый тип сертификата:
   - Если выбран сертификат закрытого типа (**Контейнер PKCS#12**), укажите файл сертификата и пароль.
   - Если выбран сертификат открытого типа (**X.509-сертификат**):
     a. укажите файл закрытого ключа (файл с расширением prk или pem);
     b. укажите пароль закрытого ключа;
     c. укажите файл открытого ключа (файл с расширением cer).
8. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для SMTP-сервера.

Выборки событий

Информация о событиях в работе Kaspersky Security Center и управляемых программ сохраняется как в базе данных Сервера администрирования, так и в системном журнале Microsoft Windows. Вы можете просматривать информацию из базы данных Сервера администрирования в рабочей области узла **Сервер администрирования** на закладке **События**.

Информация на закладке **События** представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства – Критический" содержит только записи об изменении статусов устройств на "Критический". После установки программы на закладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл.

В этом разделе

Просмотр выборки событий

► *Чтобы просмотреть выборку событий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите нужную вам выборку событий.

   Если вы хотите, чтобы события этой выборки отображались в рабочей области постоянно, нажмите на кнопку ☆ рядом с выборкой.

В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сортировать информацию в списке событий по возрастанию или убыванию данных в любой графе списка.

Настройка параметров выборки событий

► *Чтобы настроить параметры выборки событий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Откройте нужную вам выборку событий на закладке **События**.
4. Нажмите на кнопку **Свойства**.

В открывшемся окне свойств выборки событий вы можете настроить параметры выборки.

Создание выборки событий

► *Чтобы создать выборку событий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне **Новая выборка событий** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в раскрывающемся списке **Выборки событий** будет создана выборка с указанным вами именем.

По умолчанию созданная выборка событий содержит все события, хранящиеся на Сервере администрирования. Чтобы в выборке отображались только интересующие вас события, нужно настроить параметры выборки.

Экспорт выборки событий в текстовый файл

► *Чтобы экспортировать выборку событий в текстовый файл, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Нажмите на кнопку **Импорт/Экспорт**.
4. В раскрывающемся списке выберите **Экспортировать события в файл**.

В результате запустится мастер экспорта событий. Следуйте далее указаниям мастера.

Удаление событий из выборки

► *Чтобы удалить события из выборки, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **События**.
3. Выберите события, которые требуется удалить, с помощью мыши и клавиш **Shift** или **Ctrl**.
4. Удалите выбранные события одним из следующих способов:
   - В контекстном меню любого из выделенных событий выберите пункт **Удалить**.

     При выборе пункта контекстного меню **Удалить все** из выборки будут удалены все отображаемые события, независимо от того, какие из них вы предварительно выбрали для удаления.
   - По ссылке **Удалить событие**, если выбрано одно событие, или по ссылке **Удалить события**, если выбрано несколько событий, в блоке работы с выбранными событиями.

В результате выбранные события будут удалены.

Добавление программ в исключения по запросам пользователей

Если вы получаете запросы пользователей для разблокирования ошибочно заблокированных программ, вы можете создать исключение из правил Адаптивного контроля аномалий для этих программ. Такие программы больше не будут блокироваться на устройствах пользователей. Вы можете отслеживать количество запросов пользователей на закладке **Мониторинг** в рабочей области Сервера администрирования.

► *Чтобы добавить программу, заблокированную Kaspersky Endpoint Security, в исключения по запросам пользователей, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите выборку событий **Запросы пользователей**.
4. В контекстном меню запроса пользователя (или нескольких запросов пользователей), содержащих программы, которые необходимо добавить в исключения, выберите пункт **Добавить исключения**.

   Запустится мастер добавления исключений (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. 727). Следуйте шагам мастера.

Выбранные программы будут исключены из списка **Срабатывание правил в интеллектуальном режиме** (в папке **Хранилища** дерева консоли) после следующей синхронизации клиентского устройства с Сервером администрирования. Такие программы больше не будут отображаться в списке.

Настройка экспорта событий в SIEM-систему

Программа позволяет экспортировать события в работе Сервера администрирования и других программ "Лаборатории Касперского", установленных на клиентских устройствах, в SIEM-систему (SIEM – Security Information and Event Management).

► *Чтобы настроить экспорт событий в SIEM-систему, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

   Откроется окно свойств событий на разделе **Экспорт событий**.
4. Установите флажок **Автоматически экспортировать события в базу SIEM-системы**.
5. В раскрывающемся списке **SIEM-система** выберите систему, в которую нужно экспортировать события.

   Доступен экспорт событий в SIEM-системы QRadar® (LEEF-формат), ArcSight (CEF-формат), Splunk® (CEF-формат) и формат Syslog (RFC 5424). По умолчанию выбрана система ArcSight (CEF-формат).
6. Укажите адрес сервера SIEM-системы и порт для подключения к серверу в соответствующих полях.

   По кнопке **Экспортировать архив** программа экспортирует уже созданные события в базу SIEM-системы с указанной даты. По умолчанию программа экспортирует события с текущей даты.
7. Нажмите на кнопку **ОК**.

В результате после установки флажка **Автоматически экспортировать события в базу SIEM-системы** и настройки соединения с сервером программа будет автоматически экспортировать все события в работе Сервера администрирования и других программ "Лаборатории Касперского" в SIEM-систему.

Более подробную информацию об экспорте событий см. в разделе "Экспорт событий в SIEM-системы" (см. стр. 741).

Выборки устройств

Информация о состоянии устройств содержится в дереве консоли в папке **Выборки устройств**.

Информация в папке **Выборки устройств** представлена в виде списка выборок устройств. Каждая выборка включает в себя устройства, отвечающие определенным условиям. Например, выборка **Устройства со статусом "Критический"** содержит только устройства со статусом *Критический*. После установки программы папка **Выборки устройств** содержит ряд стандартных выборок. Вы можете создавать дополнительные (пользовательские) выборки устройств, экспортировать параметры выборок в файл, а также создавать выборки с параметрами, импортированными из файла.

В этом разделе

Просмотр выборки устройств

► *Чтобы просмотреть выборку устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки в раскрывающемся списке **Устройства выборки** выберите нужную вам выборку устройств.

   Если вы хотите, чтобы устройства этой выборки отображались в рабочей области постоянно, нажмите на кнопку ☆ рядом с выборкой.

В результате в рабочей области отобразится список устройств, отвечающих параметрам выборки.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных в любой из граф.

Параметры условий выборки устройств

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

- **Инвертировать условие выборки**

  Если флажок установлен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

  По умолчанию флажок снят.

Сеть

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых

данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя).

- **Windows-домен**

  Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

  - Внутри одного слова:
    - *****. Заменяет любую строку длиной 0 и более символов.

    Пример:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

    Пример:

    Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

  - Для связи нескольких слов:
    - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

    Пример:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

    - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

    Пример:

    Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

    - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-интервал**

  Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию флажок снят.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

По умолчанию флажок снят.

- **Включая дочерние подразделения**

  Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является агентом обновлений**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Есть**. В выборку будут включены устройства, являющиеся точками распространения.
  - **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Есть**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано**. Критерий не применяется.

- **Время последнего соединения с Сервером администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если флажок установлен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если флажок снят, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию флажок снят.

- **Устройство видимо в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Есть**. Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

Программа

В разделе **Программа** можно настроить критерии включения устройств в выборку на основании выбранной управляемой программы:

- **Название программы**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав

выборки при поиске по наименованию программы "Лаборатории Касперского".

В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center 10**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Есть**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Установлена программа защиты**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

- **Есть**. Программа включает в выборку устройства, на которых установлена программа безопасности.
- **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
- **Значение не выбрано**. Критерий не применяется.

Операционная система

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы:

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы (X.Y.)**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Статус устройства

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемой программы:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический*, *Предупреждение*.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический*, *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

В разделе **Компоненты защиты** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию флажок снят.

- **Количество записей в базах**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

  По умолчанию флажок снят.

- **Время последнего поиска вирусов**

  Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого антивирусная проверка выполнялась в последний раз.

  По умолчанию флажок снят.

- **Количество найденных вирусов**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию флажок снят.

Реестр программ

В разделе **Реестр программ** можно настроить критерии включения устройств в выборку в зависимости от того, какие программы на них установлены:

- **Название программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Производитель**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Статус программы**

Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если флажок установлен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки флажка названия полей ввода **Название программы** и **Версия программы** меняются на **Имя обновления** и **Версия обновления**.

  По умолчанию флажок снят.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

  В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применять к устройствам без выбранных тегов**

Если флажок установлен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если флажок снят, критерий не применяется.

По умолчанию флажок снят.

Реестр оборудования

В разделе **Оборудование** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Производитель**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  Имя устройства в Windows-сети. Устройство с указанным именем будет включено в

выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

  Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Производитель устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

  Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Виртуальные машины

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Есть**. Искомые устройства должны являться виртуальными машинами.
  - **Нет**. Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Есть**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Уязвимости и обновления

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Windows Update:

- **WUA переключен на Сервер администрирования**

  В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

  - **Есть**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
  - **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если флажок установлен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если флажок установлен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Описания статусов от управляемой программы

В разделе **Описания статусов от управляемой программы** можно настроить критерии включения устройств в выборку по описаниям статусов устройств от управляемой программы:

- **Описание статуса устройства**

  Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

Статусы компонентов управляемых программ

В разделе **Статусы компонентов управляемых программ** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу защиты данных от утечек (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

Экспорт параметров выборки устройств в файл

► *Чтобы экспортировать параметры выборки устройств в текстовый файл, выполните следующие*

действия:

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Экспортировать параметры**.
3. В открывшемся окне **Сохранить как** задайте имя файла для экспорта параметров выборки, укажите папку, в которую будет сохранен файл, и нажмите на кнопку **Сохранить**.

Параметры выборки устройств будут сохранены в указанный файл.

Создание выборки устройств

► *Чтобы создать выборку устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Создать выборку**.
3. В открывшемся окне **Новая выборка устройств** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в дереве консоли в папке **Выборки устройств** будет создана новая папка с указанным вами именем. По умолчанию созданная выборка устройств содержит все устройства, входящие в группы администрирования того Сервера, под управлением которого создана выборка. Чтобы в выборке отображались только интересующие вас устройства, нужно настроить параметры выборки по кнопке **Свойства выборки**.

Создание выборки устройств по импортированным параметрам

► *Чтобы создать выборку устройств по импортированным параметрам, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Импортировать**.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать параметры выборки. Нажмите на кнопку **Открыть**.

В результате в папке **Выборки устройств** будет создана выборка **Новая выборка**. Параметры новой выборки параметры импортированы из указанного файла.

Если в папке **Выборки устройств** уже существует выборка с названием **Новая выборка**, к имени созданной выборки будет добавлено окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► *Чтобы удалить устройства из групп администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. Выберите устройства, которые требуется удалить, с помощью клавиш **Shift** или **Ctrl**.
3. Удалите выбранные устройства из групп администрирования одним из следующих способов:
   - В контекстном меню любого из выделенных устройств выберите пункт **Удалить**.
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Удалить из группы**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Типы событий

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования, Сервере iOS MDM и Сервере мобильных устройств Exchange ActiveSync. Типы событий, которые возникают в программах "Лаборатории Касперского", в этом разделе не перечислены.

В этом разделе

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Kaspersky Security Center, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

Можно изменить время хранения событий:

- Консоль администрирования: Настройка времени хранения события

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Критическое событие**.

Таблица 45. Критические события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено.	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц (см. раздел "О лицензионном сертификате" на стр. 255), охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищенны. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один активный ключ или действительный код активации на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий при превышении лицензионного ограничения (см. раздел "События превышения лицензионного ограничения" на стр. 266).	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака.	26 (для компонента Защита от файловых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 559). • Создайте более строгую политику (см. раздел "Активация политики по событию "Вирусная атака"" на стр. 336), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 318), которая будет запускаться при возникновении этого события.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака.	27 (для компонента Защита от почтовых угроз)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 559). • Создайте более строгую политику (см. раздел "Активация политики по событию "Вирусная атака"" на стр. 336), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 318), которая будет запускаться при возникновении этого события.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Вирусная атака.	28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 559). • Создайте более строгую политику (см. раздел "Активация политики по событию "Вирусная атака"" на стр. 336), которая будет активирована, или создайте задачу (см. раздел "Создание задачи" на стр. 318), которая будет запускаться при возникновении этого события.	180 дней
Устройство стало неуправляемым.	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Статус устройства "Критический".	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 599) при выполнении которых, статус устройства изменяется на *Критический*.	180 дней
Файл ключа в черном списке.	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в черный список. Обратитесь в Службу технической поддержки (см. стр. 939) для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности.	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky Security Center начинает работать в режиме базовой функциональности (см. раздел "Об ограничениях базовой функциональности" на стр. 259), без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: • Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky Security Center (добавьте действительный код активации или активный лицензионный ключ на Сервер администрирования). • Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней
Срок действия лицензии истекает.	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Информация будет добавлена в ближайшее время.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата истек.	4132	KLSRV_CERTIFICATE_EXPIRED	Информация будет добавлена в ближайшее время.	180 дней
Обновления модулей программ "Лаборатории Касперского" отозваны.	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Kaspersky Security Center и не относится к модулям управляемых программ "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней

См. также:

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Отказ функционирования**.

Таблица 46. События отказа функционирования Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка времени выполнения.	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных программ превышено ограничение числа установок.	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами программ сторонних производителей, и если количество установок превысило заданное в ключе программы стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите программу стороннего производителя с устройств, на которых она не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять ключами программ сторонних производителей, используя функциональность групп лицензионных программ (см. раздел "Управление ключами для групп лицензионных программ" на стр. 399). В группу лицензионных программ входят программы сторонних производителей, отвечающие заданным вами критериям.	180 дней
Не удалось выполнить опрос облачного сегмента.	4143	KLSRV_KLCLOUD_SCAN_ERROR	Информация будет добавлена в ближайшее время.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось выполнить копирование обновлений в заданную папку.	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверьте, не были ли изменены имя пользователя и / или пароль к папке (к папкам). • Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и программных модулей (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. 362).	180 дней
Нет свободного места на диске.	4107	KLSRV_DISK_FULL	Информация будет добавлена в ближайшее время.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Недоступна папка общего доступа.	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна (см. раздел "Задание папки общего доступа" на стр. 183). Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и / или пароль к папке. • Проверьте подключение к сети.	180 дней
Недоступна информационная база Сервера администрирования.	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Нет свободного места в информационной базе Сервера администрирования.	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования.
			Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна.
			Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие:
			• Вы используете SQL Server Express Edition:
			  • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных.
			  • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования.
			  • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.
			• Вы используете СУБД, отличную
				180 дней

См. также:

События предупреждения Сервера администрирования

В следующей таблице приведены события Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Предупреждение**.

Таблица 47. События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено.	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц (см. раздел "О лицензионном сертификате" на стр. 255) одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищенны. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один активный ключ или действительный код активации на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий при превышении лицензионного ограничения (см. раздел "События превышения лицензионного ограничения" на стр. 266).	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Устройство долго не проявляет активности в сети.	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Информация будет добавлена в ближайшее время.	90 дней
Конфликт имен устройств.	4102	KLSRV_EVENT_HOSTS_CONFLICT	Информация будет добавлена в ближайшее время.	90 дней
Статус устройства "Предупреждение".	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия (см. раздел "Настройка переключения статусов устройств" на стр. 599) при выполнении которых, статус устройства изменяется на *Предупреждение*.	90 дней
Для одной из групп лицензионных программ скоро будет превышено ограничение числа установок.	4127	KLSRV_INVLICPROD_FILLED	Информация будет добавлена в ближайшее время.	90 дней
Сертификат запрошен.	4133	KLSRV_CERTIFICATE_REQUESTED	Информация будет добавлена в ближайшее время.	90 дней
Сертификат удален.	4134	KLSRV_CERTIFICATE_REMOVED	Информация будет добавлена в ближайшее время.	90 дней
Срок действия APNs-сертификата истек.	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Информация будет добавлена в ближайшее время.	90 дней
Срок действия APNs-сертификата истекает.	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Информация будет добавлена в ближайшее время.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить GCM-сообщение на мобильное устройство.	4138	KLSRV_GCM_DEVICE_ERROR	Информация будет добавлена в ближайшее время.	90 дней
HTTP ошибка при отправке GCM сообщения на GCM сервер.	4139	KLSRV_GCM_HTTP_ERROR	Информация будет добавлена в ближайшее время.	90 дней
Не удалось отправить GCM-сообщение на GCM сервер.	4140	KLSRV_GCM_GENERAL_ERROR	Информация будет добавлена в ближайшее время.	90 дней
Мало свободного места на диске.	4105	KLSRV_NO_SPACE_ON_VOLUMES	Информация будет добавлена в ближайшее время.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Мало свободного места в информационной базе Сервера администрирования.	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать.
			Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие:
			• Вы используете SQL Server Express Edition:
			  • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных.
			  • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования.
			  • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера
				90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Разорвано соединение с подчиненным Сервером администрирования.	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Информация будет добавлена в ближайшее время.	90 дней
Разорвано соединение с главным Сервером администрирования.	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Информация будет добавлена в ближайшее время.	90 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN.	7719	KSNPROXY_STARTED_CON_CHK_FAILED	Информация будет добавлена в ближайшее время.	90 дней
Зарегистрированы новые обновления модулей программ "Лаборатории Касперского".	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Информация будет добавлена в ближайшее время.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Началось удаление событий из базы данных, так как превышено ограничение числа событий.	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. 557). Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Удалены события из базы данных, так как превышено ограничение числа событий.	4146	KLSRV_EVP_DB_TRUNCATED	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. 557). Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	90 дней
Срок действия лицензии истекает.	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Информация будет добавлена в ближайшее время.	90 дней

См. также:

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Информационное сообщение**.

Таблица 48. Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Ключ использован более чем на 90%.	4097	KLSRV_EV_LICENSE_CHECK_90	30 дней
Найдено новое устройство.	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 дней
Устройство автоматически добавлено в группу.	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 дней
Устройство удалено из группы: долгое отсутствие активности в сети.	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 дней
Для одной из групп лицензионных программ число разрешенных установок исчерпано более чем на 95%.	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 дней
Появились файлы для отправки на анализ в "Лабораторию Касперского".	4131	KLSRV_APS_FILE_APPEARED	30 дней
Регистрационный GCM-идентификатор мобильного устройства изменен.	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней
Обновления успешно скопированы в заданную папку.	4122	KLSRV_UPD_REPL_OK	30 дней
Установлено соединение с подчиненным Сервером администрирования.	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней
Установлено соединение с главным Сервером администрирования.	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней
Базы обновлены.	4144	KLSRV_UPD_BASES_UPDATED	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно.	7718	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN был остановлен.	7720	KSNPROXY_STOPPED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Аудит: Подключение к Серверу администрирования.	4147	KLAUD_EV_SERVERCONNECT	30 дней
Аудит: Изменение объекта.	4148	KLAUD_EV_OBJECTMODIFY	30 дней
Аудит: Изменение статуса объекта.	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней
Аудит: Изменение параметров группы.	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней

События отказа функционирования Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Отказ функционирования**.

Таблица 49. События отказа функционирования Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Ошибка при установке исправления.	7702	KLNAG_EV_PATCH_INSTALL_ERROR	События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 457) прошла неуспешно. Событие не относится к обновлениям управляемых программ "Лаборатории Касперского". Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновления стороннего производителя.	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 257), и если обновление программного обеспечения сторонних производителей (см. раздел "Обновления программного обеспечения" на стр. 427) прошло неуспешно. Проверьте, корректна ли ссылка на программу стороннего производителя. Прочтите описание события.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить обновления Центра обновления Windows.	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были неуспешными. Настройте обновления Microsoft Windows в политике Агента администрирования (см. раздел "Настройка обновлений Windows в политике Агента администрирования" на стр. 454). Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно.	30 дней

См. также:

События предупреждения Агента администрирования .....
Информационные события Агента администрирования.....

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Предупреждение**.

Таблица 50. События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установка обновления программных модулей завершена с предупреждением.	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего ПО завершена с предупреждением.	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 дней
Установка обновления стороннего ПО отложена.	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 дней
Произошел инцидент.	549	GNRL_EV_APP_INCIDENT_OCCURED	30 дней
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN.	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 дней

См. также:

События отказа функционирования Агента администрирования.....519

Информационные события Агента администрирования.....523

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Информационное событие**.

Таблица 51. Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Обновление программных модулей успешно установлено.	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления программных модулей.	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлена программа.	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Программа удалена.	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлена наблюдаемая программа.	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Установлена наблюдаемая программа.	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Установлена сторонняя программа.	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Новое устройство добавлено.	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено.	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено устройство.	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано.	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан.	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен.	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: программа была запущена.	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: предоставлен.	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней
Совместный доступ к рабочему столу Windows: завершен.	7716	KLUSRLOG_EV_WDS_END	30 дней
Установка обновления стороннего ПО завершена успешно.	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО.	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно.	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN был остановлен.	7720	KSNPROXY_STOPPED	30 дней

См. также:

События отказа функционирования Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM Kaspersky Security Center, объединенные по уровню важности **Отказ функционирования**.

Таблица 52. События отказа функционирования Сервера iOS MDM

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Не удалось запросить список профилей.		PROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить профиль.		INSTALLPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить профиль.		REMOVEPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список provisioning-профилей.		PROVISIONINGPROFILELIST_COMMAND_FAILED	30 дней
Не удалось установить provisioning-профиль.		INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось удалить provisioning-профиль.		REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 дней
Не удалось запросить список цифровых сертификатов.		CERTIFICATELIST_COMMAND_FAILED	30 дней
Не удалось запросить список установленных программ.		INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось запросить общую информацию о мобильном устройстве.		DEVICEINFORMATION_COMMAND_FAILED	30 дней
Не удалось запросить информацию о безопасности.		SECURITYINFO_COMMAND_FAILED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Не удалось заблокировать мобильное устройство.		DEVICELOCK_COMMAND_FAILED	30 дней
Не удалось очистить пароль.		CLEARPASSCODE_COMMAND_FAILED	30 дней
Не удалось удалить данные мобильного устройства.		ERASEDEVICE_COMMAND_FAILED	30 дней
Не удалось установить приложение.		INSTALLAPPLICATION_COMMAND_FAILED	30 дней
Не удалось установить код погашения для приложения.		APPLYREDEMPTIONCODE_COMMAND_FAILED	30 дней
Не удалось запросить список управляемых приложений.		MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 дней
Не удалось удалить управляемое приложение.		REMOVEAPPLICATION_COMMAND_FAILED	30 дней
Параметры роуминга отклонены.		SETROAMINGSETTINGS_COMMAND_FAILED	30 дней
Произошла ошибка в работе приложения.		PRODUCT_FAILURE	30 дней
Результат выполнения команды содержит неверные данные.		MALFORMED_COMMAND	30 дней
Не удалось отправить уведомление (Push Notification).		SEND_PUSH_NOTIFICATION_FAILED	30 дней
Не удалось отправить команду.		SEND_COMMAND_FAILED	30 дней
Устройство не найдено.		DEVICE_NOT_FOUND	30 дней

События предупреждения Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM Kaspersky Security Center, объединенные по уровню важности **Предупреждение**.

Таблица 53. События предупреждения Сервера iOS MDM

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Попытка подключения заблокированного мобильного устройства.		INACTICE_DEVICE_TRY_CONNECTED	30 дней
Профиль удален.		MDM_PROFILE_WAS_REMOVED	30 дней
Попытка повторного использования клиентского сертификата.		CLIENT_CERT_ALREADY_IN_USE	30 дней
Обнаружено неактивное устройство.		FOUND_INACTIVE_DEVICE	30 дней
Требуется код погашения.		NEED_REDEMPTION_CODE	30 дней
Профиль, входящий в состав политики, удален с устройства.		UMDM_PROFILE_WAS_REMOVED	30 дней

Информационные события Сервера iOS MDM

В таблице ниже приведены события Сервера iOS MDM Kaspersky Security Center, объединенные по уровню важности **Информационное сообщение**.

Таблица 54. Информационные события Сервера iOS MDM

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Подключено новое мобильное устройство.		NEW_DEVICE_CONNECTED	30 дней
Запрос списка профилей выполнен успешно.		PROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка профиля выполнена успешно.		INSTALLPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление профиля выполнено успешно.		REMOVEPROFILE_COMMAND_SUCCESSFULL	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Запрос списка provisioning-профилей выполнен успешно.		PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 дней
Установка provisioning-профиля выполнена успешно.		INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Удаление provisioning-профиля выполнено успешно.		REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 дней
Запрос списка цифровых сертификатов выполнен успешно.		CERTIFICATELIST_COMMAND_SUCCESSFULL	30 дней
Запрос списка установленных программ выполнен успешно.		INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Запрос общей информации о мобильном устройстве выполнен успешно.		DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 дней
Запрос информации о безопасности выполнен успешно.		SECURITYINFO_COMMAND_SUCCESSFULL	30 дней
Мобильное устройство успешно заблокировано.		DEVICELOCK_COMMAND_SUCCESSFULL	30 дней
Очистка пароля выполнена успешно.		CLEARPASSCODE_COMMAND_SUCCESSFULL	30 дней
Данные удалены с мобильного устройства.		ERASEDEVICE_COMMAND_SUCCESSFULL	30 дней
Установка приложения выполнена успешно.		INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Установка кода погашения для приложения прошла успешно.		APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 дней
Запрос списка управляемых приложений выполнен успешно.		MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 дней
Удаление управляемого приложения выполнено успешно.		REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 дней
Параметры роуминга применены успешно.		SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 дней

События отказа функционирования Сервера мобильных устройств Exchange ActiveSync

В таблице ниже приведены события Сервера мобильных устройств Exchange ActiveSync, объединенные по уровню важности **Отказ функционирования**.

Таблица 55. События отказа функционирования Сервера мобильных устройств Exchange ActiveSync

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Не удалось удалить данные мобильного устройства.		WIPE_FAILED	30 дней
Не удалось удалить информацию о подключении мобильного устройства к почтовому ящику.		DEVICE_REMOVE_FAILED	30 дней
Не удалось применить к почтовому ящику политику ActiveSync.		POLICY_APPLY_FAILED	30 дней
Ошибка функционирования программы.		PRODUCT_FAILURE	30 дней
Не удалось изменить состояние функциональности ActiveSync.		CHANGE_ACTIVE_SYNC_STATE_FAILED	30 дней

Информационные события Сервера мобильных устройств Exchange ActiveSync

В таблице ниже приведены события Сервера мобильных устройств Exchange ActiveSync, объединенные по уровню важности **Информационное сообщение**.

Таблица 56. Информационные события Сервера мобильных устройств Exchange ActiveSync

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Подключилось новое мобильное устройство.		NEW_DEVICE_CONNECTED	30 дней
Данные удалены с мобильного устройства.		WIPE_SUCCESSFULL	30 дней

Контроль изменения состояния виртуальных машин

Сервер администрирования хранит информацию о состоянии управляемых устройств, например, реестр оборудования и список установленных программ, параметры управляемых программ, задач и политик. Если управляемым устройством является виртуальная машина, пользователь может в любой момент восстановить ее состояние из образа виртуальной машины (snapshot), сделанного ранее. В результате информация о состоянии виртуальной машины на Сервере администрирования может стать неактуальной.

Например, в 12:00 администратор создал на Сервере администрирования политику защиты, которая в 12:01 начала действовать на виртуальной машине VM_1. В 12:30 пользователь виртуальной машины VM_1 изменил ее состояние, выполнив восстановление из образа, сделанного в 11:00.В результате этого политика защиты на виртуальной машине перестанет действовать. Однако на Сервере администрирования сохранится неактуальная информация о том, что политика защиты на виртуальной машине VM_1 продолжает действовать.

Kaspersky Security Center позволяет контролировать изменение состояния виртуальных машин.

После каждой синхронизации с устройством Сервер администрирования формирует уникальный идентификатор, который хранится как на устройстве, так и на Сервере администрирования. Перед началом следующей синхронизации Сервер администрирования сравнивает значения идентификаторов на обеих сторонах. Если значения идентификаторов не совпадают, Сервер администрирования считает виртуальную машину восстановленной из образа. Сервер администрирования сбрасывает действующие для этой виртуальной машины параметры политик и задач и отправляет на нее актуальные политики и список групповых задач.

Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

► *Чтобы отследить состояние антивирусной защиты на клиентском устройстве с помощью информации, записанной Агентом администрирования в системный реестр, выполните следующие*

действия:

1. Откройте системный реестр клиентского устройства (например, локально с помощью команды regedit в меню **Пуск → Выполнить**).
2. Перейдите в раздел:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
   ```

В результате в системном реестре отобразится информация о состоянии антивирусной защиты клиентского устройства.

Состояние антивирусной защиты соответствует значениям ключей, описанных в таблице ниже.

Таблица 57. Ключи реестра и их возможные значения

Ключ (тип данных)	Значение	Описание
`Protection_AdmServer (REG_SZ)`	Параметры Сервера администрирования	Имя Сервера администрирования, который управляет устройством.
`Protection_AvInstalled (REG_DWORD)`	отлично от 0	Программа безопасности установлена на устройстве
`Protection_AvRunning (REG_DWORD)`	отлично от 0	Постоянная защита устройства включена.
`Protection_HasRtp (REG_DWORD)`	отлично от 0	Установлен компонент постоянной защиты.
	Статус постоянной защиты:	
	0	Неизвестно.
	2	Не включена.
	3	Приостановлена.
	4	Запускается.
	5	Активна.
	6	Включена, высокий уровень (максимальная защита).
	7	Включена, используются параметры по умолчанию (рекомендуемые).
	8	Включена, используются параметры, настроенные пользователем.
	9	Сбой в работе.

Ключ (тип данных)	Значение	Описание
`Protection_LastFscan (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последней полной проверки.
`Protection_BasesDate (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) выпуска баз программы.
`Protection_LastConnected (REG_SZ)`	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последнего соединения с Сервером администрирования.

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

► *Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования, выполните следующие действия:*

1. Нажмите правой клавишей мыши на название требуемой группы администрирования.
2. В контекстном меню выберите пункт **Свойства**.

   Откроется окно свойств группы администрирования.
3. В окне свойств перейдите в раздел **Устройства**.
4. При необходимости включите или выключите следующие параметры:

   - **Уведомлять администратора, если устройство неактивно больше (сут)**

     Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

     По умолчанию параметр включен.

   - **Наследовать из родительской группы**

Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Когда флажок установлен, параметры в блоке параметров Активность устройства недоступны для изменения.

Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

По умолчанию параметр выключен.

- **Форсировать наследование для дочерних групп**

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.

5. Нажмите на кнопку **ОК**.

Ваши изменения сохранены и применены.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего (см. раздел "Иерархия политик, использование профилей политик" на стр. 329).

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис
- Множество небольших изолированных офисов

Устройства, выполняющие роль точек распространения, должны быть защищены от любого типа несанкционированного доступа, в том числе физически защищены.

В этом разделе

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных "частей" (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.
- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования версии 10 Service Pack 1 или более поздней версии в таком случае будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: Множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

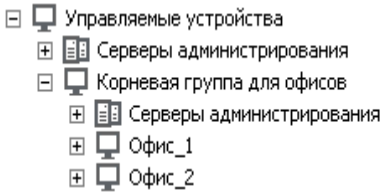


Рисунок 2: Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске (см. раздел "Требования для точки распространения" на стр. 842).

Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Назначение устройства точкой распространения и настройка шлюза соединений

Вы можете управлять устройствами организации-клиента, не имеющими прямой связи с виртуальным Сервером администрирования, через шлюз соединений.

Вы также можете вручную назначить устройство точкой распространения для группы администрирования и настроить ее как шлюз соединений в Консоли администрирования.

► *Чтобы назначить устройство точкой распространения группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** нажмите на кнопку **Добавить**.

   В результате откроется окно **Добавление точки распространения**.
4. В окне **Добавление точки распространения** выполните следующие действия:
   a. Выберите устройство, которое будет выполнять роль точки распространения, раскрыв список с помощью кнопки  , расположенной справа от кнопки **Добавить**. Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:
      - **Добавить устройство из группы**. Добавление устройства из папки **Управляемые устройства**.
      - **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**. Ввод

адреса шлюза соединений.

> Этот вариант следует использовать для добавления в качестве точки распространения устройства, защищенного сетевым экраном, поскольку его невозможно напрямую включить в группу администрирования.

При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

b. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

5. Нажмите на кнопку **ОК**.

Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

> Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу администрирования, будет автоматически назначено точкой распространения и настроено в качестве шлюза соединений.

В результате добавления точки распространения по IP-адресу Сервер администрирования обнаружит ее при очередном сканировании сети и поместит в папку **Нераспределенные устройства**. Поскольку точка распространения защищена сетевым экраном, для ее настройки требуется выполнить следующие действия.

1. Добавить это устройство в выбранную группу администрирования.
2. Снова открыть окно свойств Сервера администрирования на разделе **Точки распространения**.
3. Удалить устройство, добавленное по адресу, из списка точек распространения.
4. Добавить это же устройство из папки **Управляемые устройства** с помощью кнопки **Добавить** или **Добавить устройство из группы**.
5. В окне свойств этой точки распространения в разделе **Дополнительно** проверить, установлены ли флажки **Шлюз соединений** и **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**.

Локальная установка Агента администрирования на устройство, выбранное точкой распространения

Чтобы устройство, выбранное точкой распространения, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное точкой

распространения, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного точкой распространения, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

  Используется следующая форма записи адреса виртуального Сервера: <Полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>.

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами программа Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;
- назначает это устройство точкой распространения группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенном точкой распространения группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль точек распространения во вложенных группах администрирования, Агент администрирования можно установить удаленно. Для этого используйте точку распространения группы **Управляемые устройства** в качестве шлюза соединений.

См. также:

Локальная установка Агента администрирования .....

Программы "Лаборатории Касперского".Централизованное развертывание .....

Использование точки распространения в качестве шлюза соединений

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза

соединений можно использовать точку распространения. Точка распространения предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к точке распространения и не разрывает соединение с ней в течение всего времени работы.

Получив сигнал от Сервера администрирования, точка распространения посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При получении сигнала Агенты администрирования подключаются к точке распространения, которая передает информацию между ними и Сервером администрирования.

Рекомендуется использовать в качестве шлюза соединений выделенное устройство и назначать на один шлюз соединений не более 10 000 клиентских устройств (включая мобильные устройства).

См. также:

Назначение устройства точкой распространения и настройка шлюза соединений 536

Локальная установка Агента администрирования 138

Добавление IP-диапазонов в список проверенных диапазонов точки распространения

Вы можете добавить IP-диапазон в список опрашиваемых диапазонов точки распространения.

► *Чтобы добавить IP-диапазон в список опрашиваемых диапазонов, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.

   Откроется окно свойств точки распространения.
5. В открывшемся окне выберите раздел **Обнаружение устройств → IP-диапазоны**.
6. Установите флажок **Разрешить опрос диапазона**.
7. Нажмите на кнопку **Добавить**.

   Кнопка **Добавить** активна, если установлен флажок **Разрешить опрос диапазона**.

   Откроется окно **IP-диапазон**.
8. В окне **IP-диапазон** введите имя нового IP-диапазона (по умолчанию указано имя Новый диапазон).
9. Нажмите на кнопку **Добавить**.
10. Выполните одно из следующих действий:

- Задайте IP-диапазон начальным и конечным IP-адресом.
- Задайте IP-диапазон адресом и маской подсети.
- Нажмите на кнопку **Обзор** и добавьте подсеть из глобального списка подсетей (см. стр. 895).

11. Нажмите на кнопку **ОК**.
12. Нажмите на кнопку **ОК**, чтобы добавить диапазон с заданным именем.

Новый диапазон отобразится в списке опрашиваемых диапазонов.

Другие повседневные задачи

Этот раздел содержит рекомендации о ежедневной работе с Kaspersky Security Center.

В этом разделе

Управление Серверами администрирования

Этот раздел содержит информацию о работе с Серверами администрирования и о настройке параметров Сервера администрирования.

В этом разделе

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Добавление возможно независимо от того, доступен ли Сервер, который вы хотите сделать подчиненным, для подключения через Консоль администрирования.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Порт 13291 необходим для приема подключений от Консоли администрирования к Серверу администрирования (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 64).

Подключение Сервера администрирования в качестве подчиненного к главному Серверу

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера с подключением к главному Серверу по порту 13000. Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить Сервер администрирования, доступный для подключения через Консоль, в качестве*

подчиненного Сервера, выполните следующие действия:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Сервер администрирования** выбранной группы перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования.
6. Следуйте далее указаниям мастера.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер будет принимать подключение от подчиненного Сервера (см. раздел "Иерархия Серверов администрирования:Главный Сервер администрирования и подчиненный Сервер администрирования" на стр. 68).

Если у вас нет устройства с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования (например, если будущий подчиненный Сервер находится в удаленном офисе, а системный администратор удаленного офиса из соображений безопасности не делает доступным порт 13291 через интернет), вы все равно можете добавить подчиненный Сервер.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Консоль, в качестве подчиненного Сервера, выполните следующие действия:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для подключения от подчиненных Серверов администрирования.
2. Запишите файл сертификата будущего главного Сервера администрирования на внешнее устройство (например, съемный диск) либо перешлите системному администратору того удаленного офиса, в котором находится Сервер администрирования.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.
3. Запишите файл сертификата будущего подчиненного Сервера администрирования на внешнее устройство (например, съемный диск). Если будущий подчиненный Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса переслать вам сертификат.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.
4. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
5. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер

администрирования.

6. В рабочей области узла **Сервер администрирования** перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.

7. На первом шаге мастера (ввод адреса) оставьте поле **Адрес** пустым.

8. В окне **Выбор файла сертификата подчиненного Сервера администрирования** нажмите на кнопку **Обзор** и выберите сохраненный ранее файл сертификата подчиненного Сервера.

9. После завершения работы мастера подключитесь с помощью другой Консоли администрирования к будущему подчиненному Серверу администрирования. Если этот Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса подключиться к будущему подчиненному Серверу администрирования и выполнить на нем дальнейшие шаги.

10. В контекстном меню узла **Сервер администрирования** выберите **Свойства**.

11. В свойствах Сервера администрирования перейдите в раздел **Дополнительно** и затем в раздел **Иерархия Серверов администрирования**.

12. Установите флажок **Данный Сервер администрирования является подчиненным в иерархии**.

    Поля ввода станут доступными для ввода и редактирования.

13. В поле **Адрес главного Сервера** введите сетевое имя будущего главного Сервера администрирования.

14. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

15. Нажмите на кнопку **ОК**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Вы сможете подключаться к подчиненному Серверу через Консоль администрирования. Главный Сервер будет принимать подключение от подчиненного Сервера (см. раздел "Иерархия Серверов администрирования:Главный Сервер администрирования и подчиненный Сервер администрирования" на стр. 68).

Подключение главного Сервера администрирования к подчиненному Серверу

Вы можете добавить новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. Это целесообразно, например, если вы размещаете подчиненный Сервер в демилитаризованной зоне.

Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить новый Сервер администрирования в качестве подчиненного и подключить главный Сервер к нему по порту 13000, выполните следующие действия:*

1. Убедитесь, что порт 13000 будущего подчиненного Сервера доступен для приема подключений от главного Сервера администрирования.

2. С помощью Консоли администрирования подключитесь к будущему главному Серверу

администрирования.

3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Серверы администрирования** нужной группы администрирования перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования, и установите флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
6. Если вы подключаетесь к будущему подчиненному Серверу через прокси-сервер, на первом шаге мастера установите флажок **Использовать прокси-сервер** и введите параметры подключения.
7. Следуйте далее указаниям мастера.

Будет установлена иерархия Серверов администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера (см. раздел "Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне" на стр. 69).

См. также:

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне.....69

Иерархия Серверов администрирования: Главный Сервер администрирования и подчиненный Сервер администрирования 68

Порты, используемые Kaspersky Security Center.....56

Подключение к Серверу администрирования и переключение между Серверами администрирования

При запуске программа Kaspersky Security Center предпринимает попытку соединения с Сервером администрирования. Если в сети существует несколько Серверов администрирования, запрашивается тот Сервер, с которым было установлено соединение во время предыдущего сеанса работы программы Kaspersky Security Center.

Если программа запускается в первый раз после установки, выполняется попытка соединения с Сервером администрирования, указанным при установке Kaspersky Security Center.

После соединения с Сервером администрирования структура папок этого Сервера отображается в дереве консоли.

Если в дерево консоли добавлено несколько Серверов администрирования, вы можете переключаться

между ними.

Для работы с каждым Сервером администрирования необходима Консоль администрирования. Перед первым подключением к новому Серверу администрирования убедитесь, что на нем открыт порт 13291, по которому принимаются подключения от Консоли (см. раздел "Сервер администрирования и Консоль администрирования" на стр. 64), и все остальные порты для связи Сервера администрирования с другими компонентами Kaspersky Security Center (см. раздел "Порты, используемые Kaspersky Security Center" на стр. 56).

► *Чтобы переключиться на другой Сервер администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню узла выберите пункт **Подключиться к Серверу администрирования**.
3. В открывшемся окне **Параметры подключения** в поле **Адрес Сервера** укажите имя Сервера администрирования, к которому вы хотите подключиться. В качестве имени Сервера администрирования вы можете указать IP-адрес или имя устройства в сети Windows. При нажатии на кнопку **Дополнительно** в нижней части окна вы можете настроить параметры подключения к Серверу администрирования (см. рис. ниже).

   Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес Сервера** требуется ввести значение в формате <Имя Сервера администрирования>:<Порт>.

Пользователям, не обладающим правами на **Чтение**, будет отказано в доступе к Серверу администрирования.

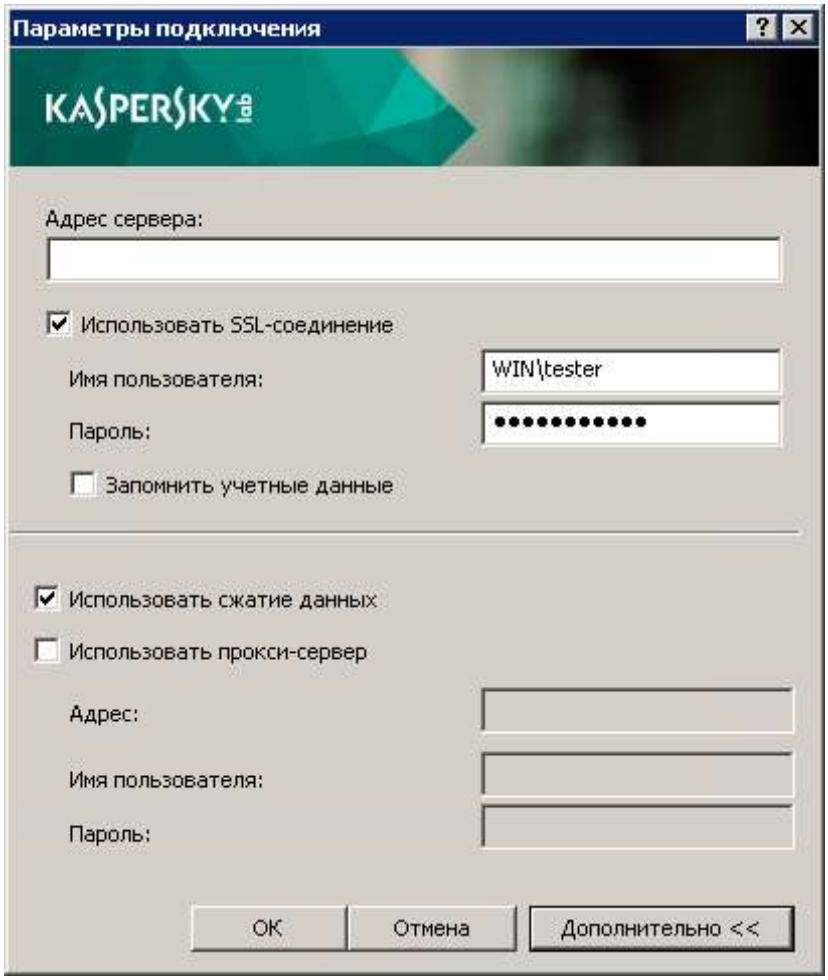


Рисунок 3: Установка соединения с Сервером администрирования

4. Нажмите на кнопку **ОК** для завершения переключения между Серверами.

После соединения с Сервером администрирования структура папок соответствующего ему узла в дереве консоли обновляется.

См. также:

Порты, используемые Kaspersky Security Center 56

Сервер администрирования и Консоль администрирования 64

Права доступа к Серверу администрирования и его объектам

При установке Kaspersky Security Center автоматически формируются группы пользователей **KLAdmins** и **KLOperators**. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы **KLAdmins** и **KLOperators** создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются в домене, в который входит Сервер администрирования, и на Сервере администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на Сервере администрирования.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений в права пользователей групп **KLAdmins** и **KLOperators** можно осуществлять при помощи стандартных средств администрирования операционной системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на чтение и выполнение. Набор прав, предоставленных группе **KLAdmins**, недоступен для изменения.

Пользователи, входящие в группу **KLAdmins**, называются *администраторами Kaspersky Security Center*, пользователи из группы **KLOperators** – *операторами Kaspersky Security Center*.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора Kaspersky Security Center предоставляются локальным администраторам устройств, на которых установлен Сервер администрирования.

Локальных администраторов можно исключать из списка пользователей, имеющих права администратора Kaspersky Security Center.

Все операции, запущенные администраторами Kaspersky Security Center, выполняются с правами учетной записи Сервера администрирования.

Для каждого Сервера администрирования в сети можно сформировать свою группу **KLAdmins**, обладающую правами только в рамках работы с этим Сервером.

Если устройства, относящиеся к одному домену, входят в группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Security Center в рамках всех этих групп администрирования. Группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Операции, запущенные администратором Kaspersky Security Center, выполняются с правами учетной записи того Сервера администрирования, для которого они запущены.

После установки программы администратор Kaspersky Security Center может выполнять следующие действия:

- изменять права, предоставляемые группам **KLOperators**;

- определять права доступа к функциям программы Kaspersky Security Center другим группам пользователей и отдельным пользователям, зарегистрированным на рабочем месте администратора;
- определять права доступа пользователей к работе в каждой группе администрирования.

Администратор Kaspersky Security Center может назначать права доступа к каждой группе администрирования или к другим объектам Сервера администрирования в разделе **Безопасность** окна свойств выбранного объекта.

Вы можете отследить действия пользователя при помощи записей о событиях в работе Сервера администрирования. Записи о событиях отображаются в узле **Сервер администрирования** на закладке **События**. Эти события имеют уровень важности **Информационное сообщение**; типы событий начинаются со слова **Аудит**.

Условия подключения к Серверу администрирования через интернет

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования, а также подключение Консоли администрирования к Серверу администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

В этом разделе

Аутентификация Сервера при подключении устройства

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

Аутентификация Сервера при подключении Консоли администрирования

При первом подключении к Серверу администрирования Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его копию локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях Консоли администрирования к этому Серверу администрирования осуществляется идентификация Сервера администрирования.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, Консоль администрирования выводит запрос на подтверждение подключения к Серверу администрирования с заданным именем и на получение нового сертификата. После подключения Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, которая

будет использоваться для идентификации Сервера в дальнейшем.

сертификат Сервера администрирования.

Две операции, аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмен информацией с устройствами, осуществляются на основании *сертификата Сервера администрирования*. Сертификат используется также для аутентификации, когда главные Серверы администрирования подключены к подчиненным Серверам администрирования.

Сертификаты, выписанные "Лабораторией Касперского"

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Сертификат Сервера администрирования действителен пять лет. Новый сертификат доставляется на Сервер администрирования за 90 дней до срока окончания действия текущего сертификата. Затем новый сертификат автоматически замещает текущий сертификат за один день до окончания его срока действия. Все Агенты администрирования на клиентских устройствах автоматически настраиваются на аутентификацию с Сервером администрирования с использованием нового сертификата.

Сертификат сторонних производителей

При необходимости можно назначить Серверу администрирования сертификат стороннего производителя. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата. При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата.

► *Чтобы заметить сертификат Сервера администрирования вручную, выполните следующие действия:*

1. Используйте утилиту klsetsrvcert для замены сертификата.

   Из командной строки выполните команду со следующим синтаксисом:

   ```
   klsetsrvcert -t <type> {-i <inputfile> [-p <password>] | -g <dnsname>} [-l <logfile>]
   ```

2. На клиентских устройствах используйте утилиту klmover (см. раздел "Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover" на стр. 587) чтобы задать новый сертификат и восстановить соединение Агента администрирования с Сервером администрирования.

   Из командной строки выполните команду со следующим синтаксисом:

   ```
   Klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>]
   ```

Сертификат Сервера администрирования заменится и Сервер аутентифицируется с Агентом

администрирования на клиентских устройствах, с использованием нового сертификата.

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. раздел "Резервное копирование и восстановление данных Сервера администрирования" на стр. 564).

Отключение от Сервера администрирования

► *Чтобы отключиться от Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел, соответствующий Серверу администрирования, от которого нужно отключиться.
2. В контекстном меню узла выберите пункт **Отключиться от Сервера администрирования**.

Добавление Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли Сервер администрирования, выполните следующие действия:*

1. В главном окне программы Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. В контекстном меню узла выберите пункт **Создать → Сервер администрирования**.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя устройства> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

Удаление Сервера администрирования из дерева консоли

► *Чтобы удалить Сервер администрирования из дерева консоли, выполните следующие действия:*

1. В дереве консоли выберите узел, соответствующий удаляемому Серверу администрирования.
2. В контекстном меню узла выберите пункт **Удалить**.

Добавление виртуального Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли виртуальный Сервер администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать виртуальный Сервер администрирования.
2. В узле Сервера администрирования выберите папку **Серверы администрирования**.

3. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

   Запустится мастер добавления виртуального Сервера администрирования.

4. В окне **Имя виртуального Сервера администрирования** укажите имя создаваемого виртуального Сервера.

   Имя виртуального Сервера администрирования не может превышать 255 символов и содержать специальные символы ("*<>?\:|).

5. В окне **Ввод адреса подключения устройств к виртуальному Серверу** укажите адрес подключения устройств.

   Адрес подключения виртуального Сервера администрирования – это сетевой адрес, по которому к нему будут подключаться устройства. Адрес подключения состоит из двух частей: сетевого адреса физического Сервера администрирования и имени виртуального Сервера, разделенных символом косой черты (слешем). Имя виртуального Сервера будет подставлено автоматически. Указанный адрес будет использоваться на этом виртуальном Сервере как адрес по умолчанию в инсталляционных пакетах Агента администрирования.

6. В окне **Создание учетной записи администратора виртуального Сервера** назначьте администратором виртуального Сервера пользователя из списка или добавьте новую учетную запись для администратора по кнопке **Создать**.

   Вы можете указать несколько учетных записей.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя виртуального Сервера>**.

Смена учетной записи службы Сервера администрирования. Утилита klsrvswch

Если вам требуется изменить учетную запись службы Сервера администрирования, заданную при установке программы Kaspersky Security Center, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования klsrvswch.

При установке Kaspersky Security Center утилита автоматически копируется в папку установки программы.

Количество запусков утилиты не ограничено.

Утилита klsrvswch позволяет менять тип учетной записи. Например, если вы используете локальную учетную запись, вы можете сменить ее на доменную учетную запись либо на управляемую учетную запись службы (и наоборот).

Windows Vista и более поздние версии Windows не позволяют использовать учетную запись LocalSystem для Сервера администрирования. В этих версиях операционных систем Windows учетная запись **LocalSystem** неактивна.

► *Чтобы изменить учетную запись службы Сервера администрирования на доменную учетную запись, выполните следующие действия:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись LocalSystem**.

В результате работы мастера учетная запись Сервера администрирования изменяется. Служба Сервера администрирования запустится под учетной записью *LocalSystem* и будет использовать ее учетные данные.

Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска службы Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

► *Чтобы изменить учетную запись службы Сервера администрирования на учетную запись пользователя или на управляемую учетную запись службы, выполните следующие действия:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись пользователя**.
3. Нажмите на кнопку **Найти**.

   Откроется окно **Выбор пользователя**.

4. В окне **Выбор пользователя** нажмите на кнопку **Типы объекта**.
5. В списке типов объекта выберите **Пользователи** (если вы хотите использовать учетную запись пользователя) или **Учетная запись для служб** (если вы хотите использовать управляемую учетную запись службы) и нажмите на кнопку **ОК**.
6. В поле для имени объекта введите имя учетной записи или часть имени и нажмите на кнопку **Проверить имена**.
7. В списке соответствующих имен выберите необходимое имя и нажмите на кнопку **ОК**.
8. Если вы выбрали **Учетные записи служб**, в окне **Пароль учетной записи**, оставьте поля **Пароль** и **Подтверждение пароля** пустыми. Если вы выбрали **Пользователи**, введите пароль для пользователя и подтвердите его.

Учетная запись службы Сервера администрирования будет запускаться под выбранной вами учетной записью.

При использовании Microsoft SQL-сервера в режиме аутентификации учетной записи пользователя средствами Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Kaspersky Security Center. По умолчанию требуется использовать схему dbo.

Решение проблем с узлами Сервера администрирования

Дерево в левой панели Консоли администрирования содержит узлы, соответствующие Серверам администрирования. Вы можете добавить в дерево консоли столько Серверов администрирования, сколько вам нужно (см. раздел "Добавление Сервера администрирования в дерево консоли" на стр. 552).

Консоль управления Microsoft Management Console (MMC) сохраняет список узлов Сервера администрирования в дереве консоли в теневую копию файла .msc. Теневая копия этого файла хранится в папке %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ на устройстве, на котором установлена Консоль администрирования. Для каждого узла Сервера администрирования в файле содержится следующая информация:

- Адрес Сервера администрирования.
- Номер порта.
- Используется ли TLS.

  Этот параметр зависит от номера порта (см. раздел "Настройка подключения Консоли администрирования к Серверу администрирования" на стр. 225), используемого для подключения Консоли администрирования к Серверу администрирования.
- Имя пользователя.
- сертификат Сервера администрирования.

Устранение неисправностей

При подключении Консоли администрирования к Серверу администрирования (см. раздел "Аутентификация Сервера при подключении Консоли администрирования" на стр. 550), сохраненный локально сертификат сравнивается с сертификатом Сервера администрирования. Если сертификаты не совпадают, в Консоли администрирования возникает ошибка. Несовпадение сертификатов может произойти, например, при замене сертификата Сервера администрирования (см. раздел "Сертификат Сервера администрирования" на стр. 551). В этом случае необходимо повторно создать узел Сервер администрирования в консоли.

► *Чтобы повторно создать узел Сервера администрирования, выполните следующие действия:*

1. Закройте окно Консоли администрирования Kaspersky Security Center.
2. Удалите файл Kaspersky Security Center 11 из папки %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.

3. Запустить Консоль администрирования Kaspersky Security Center.

   Отобразится предложение подключиться к Серверу администрирования и принять его существующий сертификат.

4. Выполните одно из следующих действий:

   - Примите существующий сертификат, нажав на кнопку **Да**.
   - Чтобы указать ваш сертификат, нажмите на кнопку **Нет** и перейдите к файлу сертификата, используемого для аутентификации Сервера администрирования.

Проблема с сертификатом решена. Вы можете использовать Консоль администрирования для подключения к Серверу администрирования.

Просмотр и изменение параметров Сервера администрирования

Вы можете настраивать параметры Сервера администрирования в окне свойств Сервера администрирования.

► *Чтобы открыть окно Свойства: Сервер администрирования,*

в контекстном меню узла Сервера администрирования в дереве консоли выберите пункт **Свойства**.

В этом разделе

Настройка общих параметров Сервера администрирования

Вы можете настраивать общие параметры Сервера администрирования в разделах **Общие**, **Параметры**, **Хранение событий**, и **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** не отображается в окне свойств Сервера администрирования, если его отображение выключено в интерфейсе Консоли администрирования.

► *Чтобы включить отображение раздела **Безопасность** в Консоли администрирования, выполните*

следующие действия:

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок **Отображать разделы с параметрами безопасности** и нажмите на кнопку **ОК**.
4. В окне с сообщением программы нажмите на кнопку **ОК**.

Раздел **Безопасность** отобразится в окне свойств Сервера администрирования.

Параметры интерфейса Консоли администрирования

Вы можете настроить параметры интерфейса Консоли администрирования для отображения или скрытия элементов управления пользовательского интерфейса, связанных со следующими функциями:

- Системное администрирование.
- Шифрование и защита данных.
- Отображать параметры контроля рабочего места.
- Управление мобильными устройствами.
- Подчиненные Серверы администрирования.
- Разделы с параметрами безопасности.

► *Чтобы настроить параметры интерфейса Консоли администрирования, выполните следующие действия:*

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок рядом с функциями, которые вы хотите отображать и нажмите на кнопку **ОК**.
4. В окне с сообщением программы нажмите на кнопку **ОК**.

Выбранные функции будут отображаться в интерфейсе Консоли администрирования.

Обработка и хранение событий на Сервере администрирования

Информация о событиях в работе программы и управляемых устройств сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, программа может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры

обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программы вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые. Несмотря на то, что Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

Просмотр журнала подключений к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

► *Чтобы настроить регистрацию событий подключения к Серверу администрирования, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить регистрацию событий подключения.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования, в разделе **Параметры подключения к Серверу администрирования**, выберите подраздел **Порты подключения**.
4. Включите параметр **Регистрация событий подключения к Серверу администрирования**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Контроль возникновения вирусных эпидемий

Kaspersky Security Center позволяет вам своевременно реагировать на возникновение угроз вирусных эпидемий. Оценка угрозы вирусной эпидемии производится путем контроля вирусной активности на устройствах.

Вы можете настраивать правила оценки угрозы вирусной эпидемии и действия в случае ее возникновения в разделе **Вирусная атака** окна свойств Сервера администрирования.

Порядок оповещения о событии *Вирусная атака* можно задать в разделе **Настройка событий** окна свойств Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. 557), в окне свойств события *Вирусная атака*.

Событие *Вирусная атака* формируется при возникновении событий *Обнаружен вредоносный объект* в работе программ безопасности. Поэтому для распознавания вирусной эпидемии информацию о событиях *Обнаружен вредоносный объект* требуется сохранять на Сервере администрирования.

Параметры сохранения информации о событии *Обнаружен вредоносный объект* задаются в политиках программ безопасности.

При подсчете событий *Обнаружен вредоносный объект* учитывается только информация с устройств главного Сервера администрирования. Информация с подчиненных Серверов администрирования не учитывается. Для каждого подчиненного Сервера параметры события *Вирусная атака* требуется настраивать индивидуально.

Ограничение трафика

Для снижения трафика в сети предусмотрена возможность ограничения скорости передачи данных на Сервер администрирования с отдельных IP-диапазонов и IP-интервалов.

Вы можете создавать и настраивать правила ограничения трафика в разделе **Трафик** окна свойств Сервера администрирования.

► *Чтобы создать правила ограничения трафика, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать правила ограничения трафика.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Трафик**.
4. Нажмите на кнопку **Добавить**.
5. В окне **Новое правило** настройте следующие параметры:

   В блоке **Интервал IP-адресов, для которых нужно ограничивать трафик** можно выбрать способ задания подсети или диапазона, для которого ограничивается скорость передачи, и указать значения параметров для выбранного способа. Выберите один из следующих способов:

- **Задать интервал адресом и маской подсети**

  Трафик ограничивается по параметрам подсети. Укажите в полях ввода адрес подсети и маску подсети для определения интервала, в пределах которого будет ограничен трафик.

  Нажмите на кнопку **Обзор**, чтобы добавить подсеть из глобального списка подсетей (см. раздел "Просмотр и изменение свойств подсети в глобальном списке подсетей" на стр. 896).

- **Задать интервал начальным и конечным IP-адресом**

  Трафик ограничивается по интервалу IP-адресов. Укажите интервал IP-адресов в полях ввода **Начальный IP-адрес** и **Конечный IP-адрес**.

  По умолчанию этот вариант выбран.

В блоке **Ограничение трафика** можно настроить следующие параметры ограничения скорости передачи данных:

- **Период**

  Временной интервал, во время которого будет действовать ограничение трафика. Границы временного интервала можно указать в полях ввода.

- **Ограничение (КБ/сек)**

  Предельное значение суммарной скорости передачи входящих и исходящих данных Сервера администрирования. Ограничение действует только в течение временного интервала, заданного в поле **Период**.

- **Ограничивать трафик на оставшееся время (КБ/сек)**

  Трафик ограничивается не только в течение интервала, указанного в поле **Период**, но и в остальное время.

  По умолчанию флажок снят. Значение поля может не совпадать со значением поля **Ограничение (КБ/сек)**.

В первую очередь правила ограничения трафика влияют на передачу файлов. Эти правила не применяются к трафику, который возникает при синхронизации между Сервером администрирования и Агентом администрирования, или между Сервером администрирования и подчиненным Сервером администрирования.

Настройка параметров Веб-сервера

Веб-сервер используется для публикации автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Вы можете настроить параметры подключения Веб-сервера к Серверу администрирования и задать сертификат Веб-сервера в разделе **Веб-сервер** окна свойств Сервера администрирования.

Работа с внутренними пользователями

Учетные записи *внутренних пользователей* используются для работы с виртуальными Серверами администрирования. В рамках функциональности программы Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Вы можете настраивать параметры учетных записей внутренних пользователей в папке **Учетные записи пользователей** дерева консоли (см. раздел "Работа с учетными записями пользователей" на стр. 639).

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

Ни в коем случае не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.
В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации.

Мастер первоначальной настройки программы создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это неочевидное требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также целесообразно сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно

с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования и ключи для лицензий окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Для уменьшения размеров резервных копий целесообразно установить флажок **Сжимать резервные копии** (**Compress backup**) в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Инсталляция Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа (тот же SQL Server или MySQL) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

В этом разделе

Использование снимка файловой системы для уменьшения времени резервного копирования

В Kaspersky Security Center 11 уменьшено по сравнению с более ранними версиями время простоя Сервера администрирования во время резервного копирования данных. Кроме того, в параметры задачи добавлена функция **Использовать моментальный снимок файловой системы для резервного копирования данных**. Эта функция позволяет дополнительно уменьшить время простоя за счет того, что утилита klbackup создает при выполнении резервного копирования теневую копию диска (это занимает несколько секунд) и одновременно производит копирование базы данных (это занимает не более нескольких минут). Создав теневую копию диска и сделав копию базы данных, klbackup снова делает Сервер администрирования доступным для соединения.

Вы можете пользоваться функцией создания снимка файловой системы только при соблюдении двух

условий:

- Папка общего доступа Сервера администрирования и папка %ALLUSERSPROFILE%\KasperskyLab находятся на одном логическом диске и локальны по отношению к Серверу администрирования.
- Внутри папки %ALLUSERSPROFILE%\KasperskyLab нет созданных вручную символических ссылок.

Не используйте функцию, если хотя бы одно из этих условий не выполняется. В ответ на попытку создать снимок файловой системы программа выдаст сообщение об ошибке.

Для использования функции необходимо иметь учетную запись с правами на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%. Учетная запись службы сервера администрирования не имеет таких прав.

► *Чтобы воспользоваться функцией создания снимка файловой системы для уменьшения времени резервного копирования, выполните следующие действия:*

1. В разделе **Задачи** выберите задачу резервного копирования.
2. В контекстном меню выберите пункт **Свойства**.
3. В отобразившемся окне свойств задачи выберите раздел **Параметры**.
4. Установите флажок **Использовать моментальный снимок файловой системы для резервного копирования данных**.
5. В полях **Имя пользователя** и **Пароль** введите имя и пароль от учетной записи, имеющей право на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%.
6. Нажмите на кнопку **Применить**.

При следующих запусках задачи резервного копирования утилита klbackup будет создавать снимки файловой системы, и время простоя Сервера администрирования во время выполнения задачи уменьшится.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – смотря по тому, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы

данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.
Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенной программы Kaspersky Security Center и, как следствие, неправильная работа программы.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Консоль администрирования.
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

В этом разделе

Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
   - По кнопке **Создать задачу** в рабочей области.

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера **Тип задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи.

Утилита резервного копирования и восстановления данных (klbackup)

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

Утилита klbackup может работать в двух режимах:

- интерактивном (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. 566);
- неинтерактивном (см. раздел "Резервное копирование и восстановление данных в неинтерактивном режиме" на стр. 568).

Резервное копирование и восстановление данных в интерактивном режиме

► *Чтобы создать резервную копию данных Сервера администрирования в интерактивном режиме, выполните следующие действия:*

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center.

   В результате запустится мастер резервного копирования и восстановления данных.

2. В первом окне мастера выберите пункт **Выполнить резервное копирование данных Сервера администрирования**.

   При установке флажка **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет сохранена только резервная копия сертификата Сервера администрирования.

   Нажмите **Далее**.

3. В следующем окне мастера укажите пароль и папку назначения для резервного копирования. Нажмите на кнопку **Далее** для выполнения резервного копирования.

4. Если вы работаете с базой данных в облачном окружении, таком как Amazon Web Services (AWS) или Microsoft Azure, заполните следующие поля в окне **Войти в онлайн-хранилище**:

   - Для AWS:
     - **Имя корзины S3**

       Имя корзины S3 (см. раздел "Подготовка корзины S3 Amazon для базы данных" на стр. 787), которое вы создали для резервной копии данных.

     - **ID ключа доступа**

       Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

       Поле доступно, если вы выбрали базу данных RDS для контейнера S3.

     - **Секретный ключ**

       Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

- Для Microsoft Azure:
  - **Имя учетной записи хранения Azure**

    Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center (см. раздел "Создание учетной записи хранения Azure" на стр. 794).

  - **Идентификатор подписки Azure**

    Вы создали подписку на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  - **Пароль Azure**

    Вы получили пароль к идентификатору приложения при создании ID приложения в Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

    Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

  - **Идентификатор приложения в Azure**

    Вы создали этот идентификатор приложения на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

    Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

  - **Имя SQL-сервера Azure**

    Имя и группа источника доступны в свойствах SQL-сервера Azure.

  - **Группа источника SQL-сервера Azure**

    Имя и группа источника доступны в свойствах SQL-сервера Azure.

  - **Ключ доступа хранилища Azure**

    Доступен в свойствах учетной записи хранения в разделе "Access Keys" (см. раздел "Работа с Azure SQL" на стр. 794). Вы можете использовать любой ключ (key1 или key2).

► *Чтобы восстановить данные Сервера администрирования в интерактивном режиме, выполните следующие действия:*

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center.

   В результате запустится мастер резервного копирования и восстановления данных.

   > Запускать утилиту klbackup необходимо под той же учетной записью, под которой был установлен Сервер администрирования

2. В первом окне мастера выберите пункт **Выполнить восстановление данных Сервера администрирования**.

   При установке флажка **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет восстановлен только сертификат Сервера администрирования.

   Нажмите **Далее**.

3. В окне мастера **Параметры восстановления**:

   - Укажите папку, содержащую резервную копию данных Сервера администрирования. Если вы работаете в облачном окружении, таком как AWS или Azure, укажите адрес хранилища.
   - Укажите пароль, введенный при резервном копировании данных.

4. Нажмите на кнопку **Далее** для восстановления данных.

   > При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если вы укажете неверный пароль, данные не будут восстановлены. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке.

См. также:

Резервное копирование и восстановление данных в неинтерактивном режиме 568

Резервное копирование и восстановление данных в неинтерактивном режиме

► *Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в неинтерактивном режиме,*

в командной строке устройства, на котором установлен Сервер администрирования, запустите утилиту

klbackup с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore]
[-password PASSWORD] [-online]
```

> Если не задать пароль в командной строке утилиты klbackup, утилита запросит его ввод интерактивно.

Описания ключей:

- `-path BACKUP_PATH` – сохранить информацию в папке BACKUP_PATH / использовать для восстановления данные из папки BACKUP_PATH (обязательный параметр).
- `-logfile LOGFILE` – сохранить отчет о копировании или восстановлении данных Сервера администрирования.

  > Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке BACKUP_PATH.

- `-use_ts` – при сохранении данных копировать информацию в папку BACKUP_PATH, во вложенную папку с именем, отображающим текущую системную дату и время операции в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`. Если ключ не задан, информация сохраняется в корне папки BACKUP_PATH.

  > При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. Обновление информации не произойдет.

  Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBackups`, то в папке `klbackup 2017-06-19 # 11-30-18`, сохранится информация о состоянии Сервера администрирования на дату 19 июня 2017 года, 11 часов 30 минут 18 секунд.

- `-restore` – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в папке BACKUP_PATH. Если ключ отсутствует, производится резервное копирование данных в папку BACKUP_PATH.
- `-Password PASSWORD` – сохранить или восстановить сертификат Сервера администрирования; для шифрования и расшифровки сертификата использовать пароль, заданный параметром PASSWORD.

  > Забытый пароль не может быть восстановлен.

- `-online`—Back up Administration Server data by creating a volume snapshot to minimize the offline time of the Administration Server. Если вы используете утилиту резервного копирования и

восстановления данных, этот параметр игнорируется.

При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если вы укажете неверный пароль, данные не будут восстановлены. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке.

Перенос Сервера администрирования на другое устройство

► *Чтобы перенести Сервер администрирования на другое устройство без смены базы данных Сервера администрирования, выполните следующие действия:*

1. Создайте резервную копию данных Сервера администрирования.
2. Установите Сервер администрирования на выбранное устройство.

   Для упрощения переноса групп администрирования желательно, чтобы адрес нового Сервера администрирования совпадал с адресом предыдущего Сервера. Адрес (имя устройства в сети Windows или IP-адрес) указывается в параметрах подключения Агента администрирования к Серверу.

3. На новом Сервере администрирования выполните восстановление данных Сервера из резервной копии.
4. Если адрес (имя устройства в сети Windows или IP-адрес) нового Сервера администрирования не совпадает с адресом предыдущего Сервера, для подключения клиентских устройств к новому Серверу создайте на предыдущем Сервере задачу смены Сервера администрирования для группы **Управляемые устройства**.

   Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено по указанному в параметрах адресу Сервера.

5. Удалите предыдущий Сервер администрирования.

► *Чтобы перенести Сервер администрирования на другое устройство со сменой базы данных Сервера администрирования, выполните следующие действия:*

1. Создайте резервную копию данных Сервера администрирования.
2. Установите новый SQL-сервер.

Для правильного переноса информации база данных на новом SQL-сервере должна иметь те же схемы сопоставления (collation), что и на предыдущем SQL-сервере.

3. Установите новый Сервер администрирования. Название баз данных предыдущего и нового SQL-серверов должны совпадать.

   Для упрощения переноса групп администрирования желательно, чтобы адрес нового Сервера администрирования совпадал с адресом предыдущего Сервера. Адрес (имя устройства в сети Windows или IP-адрес) указывается в параметрах подключения Агента администрирования к Серверу.

4. На новом Сервере администрирования выполните восстановление данных предыдущего Сервера из резервной копии.
5. Если адрес (имя устройства в сети Windows или IP-адрес) нового Сервера администрирования не совпадает с адресом предыдущего Сервера, для подключения клиентских устройств к новому Серверу создайте на предыдущем Сервере задачу смены Сервера администрирования для группы **Управляемые устройства**.

   Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено по указанному в параметрах адресу Сервера.
6. Удалите предыдущий Сервер администрирования.

Избегание конфликтов между Серверами администрирования

Если в сети имеется несколько Серверов администрирования, они могут видеть одни и те же клиентские устройства. Это может привести к тому, что, например, несколько Серверов администрирования будут выполнять удаленную установку одной и той же программы на одно устройство, а также к другим конфликтам. Чтобы избежать такой ситуации, в Kaspersky Security Center 11 можно запретить установку программы на устройство, управляемое другим Сервером администрирования (см. раздел "Установка программ с помощью мастера удаленной установки" на стр. 277).

Свойство **Под управлением другого Сервера администрирования** можно также использовать как критерий для следующих операций:

- поиск устройств (см. раздел "Поиск устройств" на стр. 865);
- выборки устройств (на стр. 481);
- правила перемещения устройств (на стр. 349);
- правила автоматического назначения тегов (см. раздел "Автоматическое назначение тегов устройствам" на стр. 606).

В Kaspersky Security Center 11 используется эвристический подход для определения, какой Сервер администрирования управляет клиентским устройством: тот, на котором вы работаете, или другой.

Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;
- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие программы "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

Эти действия можно выполнять, только если у вас есть права **Изменение** (см. раздел "Назначение прав пользователям и группам пользователей" на стр. 648) в области **Управление группами администрирования**, для групп, которыми вы хотите управлять (или для Сервера администрирования, к которому относятся эти группы).

В этом разделе

Создание групп администрирования

Иерархия групп администрирования формируется в главном окне программы Kaspersky Security Center в папке **Управляемые устройства**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center папка **Управляемые устройства** содержит только пустую

папку **Серверы администрирования**.

Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид** → **Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные и виртуальные Серверы администрирования.

Каждая созданная группа, как и папка **Управляемые устройства**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными и виртуальными Серверами администрирования этой группы. Информация о политиках, задачах этой группы, а также о входящих в ее состав устройствах отображается на соответствующих закладках в рабочей области этой группы.

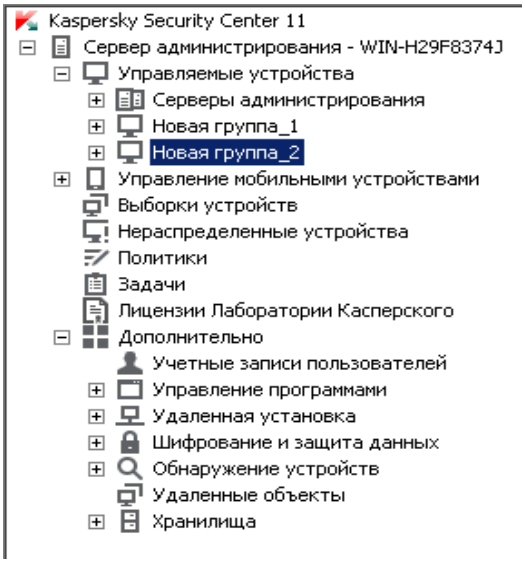


Рисунок 4: Просмотр иерархии групп администрирования

► *Чтобы создать группу администрирования, выполните следующие действия:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

   Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.
3. Запустите процесс создания группы администрирования одним из следующих способов:
   - с помощью команды контекстного меню **Создать** → **Группу**;

- по кнопке **Новая группа**, расположенной в рабочей области главного окна программы на закладке **Группы**.

4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

Программа позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► *Чтобы создать структуру групп администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи → Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Невозможно изменить название группы **Управляемые устройства**, поскольку она является встроенным элементом Консоли администрирования.

► *Чтобы переместить группу в другую папку дерева консоли, выполните следующие действия:*

1. Выберите перемещаемую группу в дереве консоли.
2. Выполните одно из следующих действий:
   - Переместите группу с помощью контекстного меню:
     1. В контекстном меню группы выберите пункт **Вырезать**.
     2. В контекстном меню группы администрирования, в которую нужно переместить выбранную группу, выберите пункт **Вставить**.

- Переместите группу с помощью главного меню программы:
  a. Выберите пункт главного меню **Действие** → **Вырезать**.
  b. Выберите в дереве консоли группу администрирования, в которую нужно переместить выбранную группу.
  c. Выберите пункт главного меню **Действие** → **Вставить**.
- Переместите группу в другую группу в дереве консоли с помощью мыши.

Удаление групп администрирования

Вы можете удалить группу администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских устройств и если для нее не сформированы задачи и политики.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

► *Чтобы удалить группу, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования.
2. Выполните одно из следующих действий:
   - в контекстном меню группы выберите пункт **Удалить**;
   - в главном меню программы выберите пункт **Действие** → **Удалить**;
   - нажмите на клавишу **DEL**.

Автоматическое создание структуры групп администрирования

Kaspersky Security Center позволяет автоматически сформировать структуру групп администрирования с помощью мастера создания структуры групп.

Мастер создает структуру групп администрирования на основе следующих данных:

- структуры доменов и рабочих групп сети Windows;
- структуры групп Active Directory;
- содержимого текстового файла, созданного администратором вручную.

При формировании текстового файла требуется соблюдать следующие правила:

- Имя каждой новой группы должно начинаться с новой строки; разделитель должен начинаться с разрыва строки. Пустые строки игнорируются.

Пример:

Офис 1

Офис 2

Офис 3

В группе назначения будут созданы три группы первого уровня иерархии.

- Имя вложенной группы следует указывать через косую черту (/).

Пример:

Офис 1/Подразделение 1/Отдел 1/Группа 1

В группе назначения будут созданы четыре вложенные друг в друга подгруппы.

- Чтобы создать несколько вложенных групп одного уровня иерархии, следует указать "полный путь к группе".

Пример:

Офис 1/Подразделение 1/Отдел 1

Офис 1/Подразделение 2/Отдел 1

Офис 1/Подразделение 3/Отдел 1

Офис 1/Подразделение 4/Отдел 1

В группе назначения будет создана одна группа первого уровня иерархии "Офис 1", в состав которой будут входить че "Подразделение 1", "Подразделение 2", "Подразделение 3", "Подразделение 4". В состав каждой из этих групп будет

Создание структуры групп администрирования с помощью мастера не нарушает целостности сети: новые группы добавляются, а не замещают существующие. Клиентское устройство не может быть включено в состав группы администрирования повторно, поскольку при перемещении устройства в группу администрирования оно удаляется из группы **Нераспределенные устройства**.

Если при создании структуры групп администрирования устройство по каким-либо причинам не было включено в состав группы **Нераспределенные устройства** (было выключено, отключено от сети), оно не будет автоматически перенесено в группу администрирования. Вы можете добавить устройства в группы администрирования вручную после завершения работы мастера.

► *Чтобы запустить автоматическое создание структуры групп администрирования, выполните следующие действия:*

1. Выберите в дереве консоли папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи → Новая**

структура групп.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Автоматическая установка программ на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки программ "Лаборатории Касперского" на вновь включенные в состав группы клиентские устройства.

► *Чтобы настроить автоматическую установку программ на новые устройства в группе администрирования, выполните следующие действия:*

1. Выберите в дереве консоли нужную вам группу администрирования.
2. Откройте окно свойств этой группы администрирования.
3. В разделе **Автоматическая установка** выберите инсталляционные пакеты, которые следует устанавливать на новые устройства.
4. Нажмите на кнопку **ОК**.

Групповые задачи созданы. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одной программы, задача установки будет создана только для последней версии программы.

Автономные пользователи

В Kaspersky Security Center предусмотрена возможность переключения Агента администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- Нахождение в подсети – изменение адреса и маски подсети.
- Нахождение в DNS-домене – изменение DNS-суффикса подсети.
- Адрес основного шлюза – изменение основного шлюза сети.
- Адрес DHCP-сервера – изменение IP-адреса DHCP-сервера в сети.
- Адрес DNS-сервера – изменение IP-адреса DNS-сервера в сети.

- Адрес WINS-сервера – изменение IP-адреса WINS-сервера в сети.
- Доступность домена Windows – изменение статуса домена Windows, к которому подключено клиентское устройство.

Такая возможность поддерживается для следующих операционных систем: Microsoft Windows XP / Windows Vista; Microsoft Windows Server 2003 / 2008.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах программы переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах программы возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

По умолчанию Агент администрирования переходит на политику для автономных пользователей, если Сервер администрирования недоступен более 45 минут.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

В этом разделе

Создание профиля подключения к Серверу администрирования для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows.

► *Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать профиль подключения Агента администрирования к Серверу.
2. Выполните одно из следующих действий:
   - Если вы хотите создать профиль подключения для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
   - Если вы хотите создать профиль подключения для выбранного устройства в составе группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:
     a. Откройте окно свойств выбранного устройства.
     b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
     c. Откройте окно свойств Агента администрирования.
3. В окне свойств в разделе **Сеть** выберите вложенный раздел **Подключение**.
4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

   По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

   В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах программы используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

   В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.
5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:
   - **Имя профиля**

     В поле ввода можно просмотреть или изменить имя профиля подключения.
   - **Адрес Сервера**

     Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.
   - **Номер порта**

     Номер порта, по которому будет выполняться подключение.
   - **Номер SSL-порта**

     Номер порта, по которому будет осуществляться подключение с использованием

SSL-протокола.

- **Использовать SSL-соединение**

  Если флажок установлен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

  По умолчанию флажок установлен.

- По ссылке **Настроить подключение через прокси-сервер** настройте параметры профиля подключения через прокси-сервер:

  - **Использовать прокси-сервер**

    Если флажок установлен, подключение к Серверу администрирования будет выполняться через прокси-сервер.

    Если флажок снят, поля ввода параметров подключения к прокси-серверу недоступны.

    По умолчанию флажок снят.

  - **Адрес**

    Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

    Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

  - **Имя пользователя** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

    Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

  - **Пароль** (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**)

    Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

- **Адрес шлюза соединений.**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим**

Если флажок установлен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. 577). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

Если флажок снят, программы будут использовать активные политики.

По умолчанию флажок снят.

- **Использовать только для получения обновлений**

  Если флажок установлен, профиль будет использоваться только при загрузке обновлений программами, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию флажок установлен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

  Если флажок установлен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

  Если флажок снят, Агент администрирования подключается к Серверу, используя исходные параметры, указанные при установке.

  Флажок доступен, если флажок **Использовать только для получения обновлений** снят.

  По умолчанию флажок снят.

6. Установите флажок **Включить автономный режим, когда Сервер администрирования недоступен**, чтобы при подключении программы, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. 577), если Сервер администрирования недоступен. В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль программы, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows.

► *Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать правило переключения Агента администрирования по описанию сетевого местоположения.
2. Выполните одно из следующих действий:
   - Если вы хотите создать правило для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
   - Если вы хотите создать правило для выбранного устройства группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:
     a. Откройте окно свойств выбранного устройства.
     b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
     c. Откройте окно свойств Агента администрирования.
3. В открывшемся окне свойств в разделе **Сеть** выберите вложенный раздел **Подключение**.
4. В блоке **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Новое описание** настройте параметры описания сетевого местоположения и правила переключения. Настройте следующие параметры описания сетевого местоположения:
   - **Имя описания сетевого местоположения**

     Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\/:|).
   - **Использовать профиль подключения**

     В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.
6. В блоке **Условия переключения** нажмите на кнопку **Добавить**, чтобы сформировать список условий описания сетевого местоположения.

   Условия правила объединяются с использованием логического оператора AND. Чтобы правило

переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В раскрывающемся списке выберите значение, соответствующее изменению характеристики сети, к которой подключено клиентское устройство:

   - **Нахождение в подсети** – изменение адреса и маски подсети.
   - **Нахождение в DNS-домене** – изменение DNS-суффикса подсети.
   - **Адрес основного шлюза** – изменение основного шлюза сети.
   - **Адрес DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
   - **Адрес DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
   - **Адрес WINS-сервера** – изменение IP-адреса WINS-сервера в сети.
   - **Доступность Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство.

8. В открывшемся окне укажите значение условия переключения Агента администрирования на другой Сервер администрирования. Название окна зависит от выбора значения на предыдущем шаге. Настройте следующие параметры условия переключения:

   - **Значение**

     В поле можно добавить одно или несколько значений для создаваемого условия.

   - **Соответствует хотя бы одному значению списка**

     Если выбран этот вариант, условие будет выполняться при любом из значений, указанных в списке **Значение**.

     По умолчанию выбран этот вариант.

   - **Не соответствует ни одному из значений списка**

     Если выбран этот вариант, условие будет выполняться, если его значение отсутствует в списке **Значение**.

9. В окне **Новое описание** настройте установите флажок **Описание активно**, чтобы включить использование нового описания сетевого местоположения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

Описания сетевого местоположения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким описаниям, будет использоваться первое из них. Вы можете изменить порядок следования правил в списке с помощью кнопок **Вверх** () и **Вниз** ().

Управление клиентскими устройствами

Этот раздел содержит информацию о работе с клиентскими устройствами.

В этом разделе

Подключение клиентских устройств к Серверу администрирования

Подключение клиентского устройства к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском устройстве.

При подключении клиентского устройства к Серверу администрирования выполняются следующие операции:

- Автоматическая синхронизация данных:
  - синхронизация списка программ, установленных на клиентском устройстве;
  - синхронизация политик, параметров программ, задач и параметров задач.
- Получение Сервером текущей информации о состоянии программ, выполнении задач и статистики работы программ.
- Доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Вы можете вручную задать интервал между соединениями.

Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Kaspersky Security Center позволяет настроить соединение клиентского устройства с Сервером администрирования таким образом, чтобы соединение не завершалось по окончании выполнения операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния программ, а Сервер администрирования не может инициировать соединение с клиентским устройством (например, соединение защищено межсетевым экраном, запрещено открывать порты на клиентском устройстве, неизвестен IP-адрес клиентского устройства). Установить неразрывное соединение клиентского устройства с Сервером администрирования можно в окне свойств устройства, в разделе **Общие** .

Рекомендуется устанавливать непрерывное соединение с наиболее важными устройствами. Общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено (до 300).

При синхронизации вручную используется вспомогательный способ подключения, при котором соединение инициирует Сервер администрирования. Перед подключением на клиентском устройстве требуется открыть UDP-порт. Сервер администрирования посылает на UDP-порт клиентского устройства запрос на соединение. В ответ на него производится проверка сертификата Сервера администрирования. Если сертификат Сервера совпадает с копией сертификата на клиентском устройстве, соединение осуществляется.

Запуск процесса синхронизации вручную используется также для получения текущей информации о состоянии программ, выполнении задач и статистике работы программ.

Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover

Если вам требуется подключить клиентское устройство к Серверу администрирования вручную, вы можете воспользоваться утилитой klmover на клиентском устройстве.

При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

► *Чтобы подключить клиентское устройство к Серверу администрирования вручную с помощью утилиты klmover,*

на устройстве запустите утилиту klmover из командной строки.

При запуске из командной строки утилита klmover в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис командной строки утилиты:

```
klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>]
```

```
[-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent]
[-dupfix]
```

Описания ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, результаты и сообщения об ошибках выводятся на экран.

- `-address <адрес сервера>` – адрес Сервера администрирования для подключения.

  В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- `-ps <м>` – номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- `-nossl` – использовать незашифрованное подключение к Серверу администрирования.

  Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.

- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

  Если ключ не используется, Агент администрирования получает сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме.

  Использование ключа может быть полезно, например, при запуске утилиты из сценария входа при регистрации пользователя.

- `-dupfix` – ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Туннелирование соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для

подключения к существующей сессии, так и для создания новой удаленной сессии.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт брандмауэром.

► *Чтобы произвести туннелирование соединения клиентского устройства с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку группы, в которую входит клиентское устройство.
2. На закладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.
4. Создайте туннель в открывшемся окне **Туннелирование соединения**.

Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять программами, установленными на нем.

Удаленное подключение к клиентскому устройству можно осуществить двумя способами:

- С помощью стандартного компонента Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

  Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

- С помощью технологии совместного доступа к рабочему столу Windows. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

  Администратор может подключиться к существующему сеансу на клиентском устройстве без

отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве будет совместный доступ к рабочему столу.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита программа сохраняет информацию о файлах на клиентском устройстве, которые открывал и / или изменял администратор (см. раздел "Аудит действий на удаленном клиентском устройстве" на стр. 592).

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.
- Kaspersky Security Center использует лицензию на Системное администрирование.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью компонента "Подключение к удаленному рабочему столу", выполните следующие действия:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Создать новую сессию RDP**.

   В результате будет запущена штатная утилита Windows mstsc.exe для подключения к удаленному рабочему столу.
3. Следуйте указаниям в открывающихся окнах утилиты.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows, выполните следующие действия:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Совместный доступ к рабочему столу**.
3. В открывшемся окне **Выбор сессии рабочего стола** выберите сеанс на клиентском устройстве, к которому требуется подключиться.

   В случае успешного подключения к клиентскому устройству рабочий стол этого устройства будет доступен в окне **Kaspersky Remote Desktop Session Viewer**.
4. Для начала взаимодействия с устройством в главном меню окна **Kaspersky Remote Desktop Session Viewer** выберите пункт **Действия** → **Интерактивный режим**.

См. также:

Варианты лицензирования Kaspersky Security Center.....257

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

► *Чтобы подключиться к устройству с помощью совместного доступа к рабочему столу Windows, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства** на закладке **Устройства**.

   В рабочей области папки отображается список устройств.

2. В контекстном меню устройства, к которому вы хотите подключиться, выберите пункт **Подключиться к устройству** → **Совместный доступ к рабочему столу Windows**.

   Откроется окно **Выбор сессии рабочего стола**.

3. В окне **Выбор сессии рабочего стола** выберите сессию рабочего стола, которая будет использоваться для подключения к устройству.

4. Нажмите на кнопку **ОК**.

Будет выполнено подключение к устройству.

Настройка перезагрузки клиентского устройства

В ходе работы, установки или удаления Kaspersky Security Center может потребоваться перезагрузка клиентского устройства. Вы можете настроить параметры перезагрузки только для устройств под управлением Windows.

► *Чтобы настроить перезагрузку клиентского устройства, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить перезагрузку.
2. В рабочей области группы выберите закладку **Политики**.
3. В списке политик выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Управление перезагрузкой**.
5. Выберите действие, которое нужно выполнять, если потребуется перезагрузка устройства:
   - Выберите **Не перезагружать операционную систему**, чтобы запретить автоматическую перезагрузку.
   - Выберите **При необходимости перезагрузить операционную систему автоматически**, чтобы

разрешить автоматическую перезагрузку.

- Выберите **Запрашивать у пользователя**, чтобы включить запрос на перезагрузку у пользователя.

Вы можете указать периодичность запроса на перезагрузку, включить принудительную перезагрузку и принудительное закрытие программ в заблокированных сессиях на устройстве, установив соответствующие флажки и интервалы.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате перезагрузка операционной системы устройства будет настроена.

Аудит действий на удаленном клиентском устройстве

Программа позволяет выполнять аудит действий администратора на удаленных клиентских устройствах под управлением Windows. В ходе аудита программа сохраняет информацию о файлах на устройстве, которые открывал и / или изменял администратор. Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

► *Чтобы включить аудит действий на удаленном клиентском устройстве, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить аудит действий администратора.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Совместный доступ к рабочему столу Windows**.
5. Установите флажок **Включить аудит**.
6. В списках **Маски файлов, чтение которых нужно отслеживать** и **Маски файлов, изменение которых нужно отслеживать** добавьте маски файлов, действия с которыми нужно отслеживать в ходе аудита.

   По умолчанию программа отслеживает действия с файлами с расширениями .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, and .pdf.
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу будет настроен.

Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке Агента администрирования на удаленном устройстве (например, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- в базе событий Kaspersky Security Center.

Проверка соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет проверять соединение клиентского устройства с Сервером администрирования автоматически или вручную.

Автоматическая проверка соединения осуществляется на Сервере администрирования. Проверка соединения вручную осуществляется на устройстве.

В этом разделе

Автоматическая проверка соединения клиентского устройства с Сервером администрирования

► *Чтобы запустить автоматическую проверку соединения клиентского устройства с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, в которую входит устройство.
2. В рабочей области группы администрирования на закладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Проверить доступность устройства**.

В результате открывается окно, содержащее информацию о доступности устройства.

Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk.

При установке на устройство Агента администрирования утилита klnagchk автоматически копируется в папку установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет

следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты, либо выводит информацию на экран.
- Предпринимает попытку установить соединение Агента администрирования с Сервером администрирования.

  Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

► *Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,*

на устройстве запустите утилиту klnagchk из командной строки.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>]
[-restart]
```

Описания ключей:

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.
- `-sp` – вывести пароль для аутентификации пользователя на прокси-сервере.

  Параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.
- `-savecert <имя файла>` – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.
- `-restart` – перезапустить Агент администрирования после завершения работы утилиты.

Проверка времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Время последнего подключения** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

Идентификация клиентских устройств на Сервере администрирования

Идентификация клиентских устройств осуществляется на основании их имен. Имя устройства является уникальным среди всех имен устройств, подключенных к Серверу администрирования.

Имя устройства передается на Сервер администрирования либо при опросе сети Windows и обнаружении в ней нового устройства, либо при первом подключении к Серверу администрирования установленного на устройство Агента администрирования. По умолчанию имя совпадает с именем устройства в сети Windows (NetBIOS-имя). Если на Сервере администрирования уже зарегистрировано устройство с таким именем, то к имени нового устройства будет добавлено окончание с порядковым номером, например: **<Имя>-1**, **<Имя>-2**. Под этим именем устройство включается в состав группы администрирования.

Перемещение устройств в состав группы администрирования

Устройства можно перемещать из одной группы администрирования в другую только при наличии прав (см. раздел "Назначение прав пользователям и группам пользователей" на стр. 648) **Изменение** в области **Управление группами администрирования** как для исходных, так и для целевых групп администрирования (или для Сервера администрирования, к которым принадлежат эти группы).

► *Чтобы включить одно или несколько устройств в состав выбранной группы администрирования, выполните следующие действия:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой будут включены клиентские устройства.

   Если вы хотите включить устройства в состав группы **Управляемые устройства**, этот шаг можно пропустить.
3. В рабочей области выбранной группы администрирования на закладке **Устройства** запустите процесс включения устройств в группу одним из следующих способов:
   - Добавьте устройства в группу по кнопке **Переместить устройства в группу** в блоке работы со списком устройств.
   - В контекстном меню списка устройств выберите **Создать** → **Устройство**.

   В результате запустится мастер перемещения устройств. Следуя его указаниям, определите способ перемещения устройств в группу и сформируйте список устройств, включаемых в состав группы.

   Если вы формируете список устройств вручную, в качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя. Вручную в список устройств могут быть перемещены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Для импорта списка устройств из файла требуется указать файл в формате TXT с перечнем адресов добавляемых устройств. Каждый адрес должен располагаться в отдельной строке.

После завершения работы мастера выбранные устройства включаются в состав группы администрирования

и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Можно переместить устройство в выбранную группу администрирования, перетащив его мышью из папки **Нераспределенные устройства** в папку группы администрирования.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу смены Сервера администрирования одним из следующих способов:
   - Если требуется сменить Сервер администрирования для устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание групповой задачи" на стр. 318).
   - Если требуется сменить Сервер администрирования для устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. 320).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Смена Сервера администрирования**.
3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи **Смена Сервера администрирования** отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в онлайн-справке Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.1.0/ru-RU/127971.htm.

Кластеры и массивы серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что программа, установленная на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера. Кластер будет добавлен как отдельный объект в папке **Управляемые устройства** в дереве консоли со значком  .

Можно выделить несколько типичных свойств кластера:

- Кластер и любой из его узлов всегда располагаются в одной группе администрирования.
- Если администратор попытается переместить какой-либо узел кластера, то узел вернется в исходное местоположение.
- Если администратор попытается переместить кластер в другую группу, то все его узлы также переместятся вместе с ним.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

► *Чтобы удаленно управлять клиентскими устройствами, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу управления устройствами одним из следующих способов:
   - Если требуется включить, выключить или перезагрузить устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. 318).
   - Если требуется включить, выключить или перезагрузить устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. 320).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Управление устройствами**.
3. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

Доступ к локальным задачам и статистике, флажок "Не разрывать соединение с Сервером администрирования"

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами

и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации (по умолчанию 15 минут) задается в политике Агента администрирования. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Если подключение по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции не могут быть выполнены без досрочного подключения Агента администрирования к Серверу: запуск и остановка локальных задач, получение статистики управляемой программы (программы безопасности или Агента администрирования), создание тоннеля и прочее. Для решения этой проблемы в свойствах управляемого устройства (раздел **Общие**) нужно установить флажок **Не разрывать соединение с Сервером администрирования**. Общее количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Принудительная синхронизация

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. Когда Kaspersky Security Center 11 выполняет эту команду, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

О расписании соединений

В окне свойств политики Агента администрирования в разделе **Подключения** во вложенном разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования.

Подключаться при необходимости. Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

Подключаться в указанные периоды. Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Отправка сообщения пользователям устройств

► *Чтобы отправить сообщение пользователям устройств, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Создайте задачу отправки сообщения пользователям устройств одним из следующих способов:
   - Если требуется отправить сообщение пользователям клиентских устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание групповой задачи" на стр. 318).
   - Если требуется отправить сообщение пользователям устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. 320).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне Тип задачи мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center 11**, раскройте папку **Дополнительно** и выберите задачу **Сообщение для пользователя**. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными** записями пользователей (см. раздел "Рассылка сообщений пользователям" на стр. 652).
4. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными записями пользователей** (см. раздел "Рассылка сообщений пользователям" на стр. 652).

Работа с программой Kaspersky Security для виртуальных сред

Kaspersky Security Center поддерживает возможность подключения виртуальных машин к Серверу администрирования. Управление виртуальными машинами осуществляется с помощью программы Kaspersky Security для виртуальных сред 4.0. Подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0*.

Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► *Чтобы изменить статус устройства на* Критический*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Критический"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

► *Чтобы изменить статус устройства на* Предупреждение*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Предупреждение"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением `Более 7 дней` клиентскому устройству присваивается статус *Предупреждение*, а со значением `Более 14 дней` – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

Таблица 58. Условия присвоения статусов устройству

Условие	Описание условия	Возможные значения
Не установлена программа безопасности.	Агент администрирования установлен на устройстве, но не установлена программа безопасности.	• Флажок установлен. • Флажок снят.

Условие	Описание условия	Возможные значения
Найдено много вирусов.	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0
Уровень постоянной защиты отличается от уровня, установленного администратором.	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вирусов.	Устройство видимо в сети и на устройстве установлена программа безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня
Базы устарели.	Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня

Условие	Описание условия	Возможные значения
Давно не подключался.	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня
Есть активные угрозы.	Количество необработанных объектов в папке **Необработанные файлы** превышает указанное значение.	Более чем 0 штук
Требуется перезагрузка.	Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут
Установлены несовместимые программы.	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы.	• Флажок снят. • Флажок установлен.

Условие	Описание условия	Возможные значения
Обнаружены уязвимости в программах.	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в программах с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если нельзя закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии скоро истечет.	Устройство видимо в сети, но срок действия лицензии истек.	• Флажок снят. • Флажок установлен.
Срок действия лицензии скоро истечет	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача Поиск уязвимостей и требуемых обновлений больше указанного времени.	Более 1 дня
Указанный статус шифрования.	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.

Условие	Описание условия	Возможные значения
Параметры мобильного устройства не соответствуют политике.	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Флажок снят. • Флажок установлен.
Есть необработанные инциденты.	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Флажок снят. • Флажок установлен.
Определяемый программой.	Статус устройства определяется управляемой программой.	• Флажок снят. • Флажок установлен.
На устройстве заканчивается дисковое пространство.	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ

Условие	Описание условия	Возможные значения
Контроль над устройством потерян.	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Флажок снят. • Флажок установлен.
Выключена защита.	Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени.	Более чем 0 минут
Не запущена программа безопасности.	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Флажок снят. • Флажок установлен.

►

См. также:

Настройка общих параметров Сервера администрирования 556

Назначение тегов устройствам и просмотр назначенных тегов

Kaspersky Security Center позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Ручное назначение тегов устройству выполняется в свойствах устройства и может понадобиться, когда необходимо отметить отдельное устройство. Автоматическое назначение тегов выполняется Сервером администрирования в соответствии с заданными правилами назначения тегов.

В свойствах Сервера администрирования вы можете настроить автоматическое назначение тегов устройствам, управляемым этим Сервером администрирования. Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве программам и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы Windows, назначается тег *Win*. Затем можно использовать этот тег при создании выборки

устройств, чтобы отобрать устройства, работающие под управлением операционной системы Windows, и назначить им задачу.

Вы также можете использовать теги в качестве условия для активации профиля политики на управляемом устройстве, чтобы определенные профили политик применялись только на устройствах, имеющих определенные теги. Например, если в группе администрирования *Пользователи* появляется устройство с тегом *Курьер* и по тегу *Курьер* настроена активация соответствующего профиля политики, то к этому устройству будет применяться не сама политика, созданная для группы *Пользователи*, а ее профиль. Профиль политики может разрешить на этом устройстве запуск отдельных программ, которые запрещено запускать в рамках политики.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства. Каждое правило назначения тегов можно включить или выключить. Если правило включено, оно применяется к устройствам, управляемым Сервером администрирования. Если правило не нужно, но может понадобиться в дальнейшем, то нет необходимости его удалять; достаточно снять флажок **Включить правило**. При этом правило выключается и не выполняется до тех пор, пока флажок **Включить правило** не будет установлен. Отключение правила без удаления может потребоваться, если это правило необходимо временно исключить из списка правил назначения тегов, а потом опять включить.

В этом разделе

Автоматическое назначение тегов устройствам

Вы можете создавать и изменять правила автоматического назначения тегов в окне свойств Сервера администрирования.

► *Чтобы автоматически назначить теги устройствам, выполните следующие действия:*

1. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется задать правила назначения тегов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Правила назначения тегов**.
4. В разделе **Правила назначения тегов** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
5. В окне **Новое правило** настройте общие свойства правила:
   - Укажите имя правила.

Имя правила не может превышать 255 символов и содержать специальные символы ("*<>?\:|).

- Включите или выключите правило с помощью флажка **Включить правило**.

  По умолчанию флажок **Включить правило** установлен.

- В поле **Тег** введите название тега.

  Название тега не может превышать 255 символов и содержать специальные символы ("*<>?\:|).

6. В разделе **Условия** нажмите на кнопку **Добавить**, чтобы добавить новое условие, или нажмите на кнопку **Свойства**, чтобы изменить существующее условие.

   Откроется окно мастера создания условия для правила автоматического назначения тегов.

7. В окне **Условия назначения тега** установите флажки для тех условий, которые должны влиять на назначения тега. Можно выбрать несколько условий.

8. В зависимости от того, какие условия назначения тега вы выбрали, мастер покажет окна для настройки соответствующих условий. Настройте срабатывание правила по следующим условиям:

   - **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону).
   - **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
   - **Программы** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
   - **Виртуальные машины** – принадлежность устройства к разным типам виртуальных машин.
   - **Реестр программ** – наличие на устройстве программ различных производителей.

9. После настройки условия введите название условия и завершите работу мастера.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий. Добавленные условия отображаются в разделе **Условия** окна свойств правила.

10. Нажмите на кнопку **ОК** в окне **Новое правило** и на кнопку **ОК** в окне свойств Сервера администрирования.

Созданные правила выполняются на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

Просмотр и настройка тегов, назначенных устройству

Вы можете просмотреть список всех тегов, назначенных устройству, а также перейти к настройке правил автоматического назначения тегов в окне свойств устройства.

► *Чтобы просмотреть и настроить назначенные устройству теги, выполните следующие действия:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** выберите устройство, для которого вы хотите посмотреть назначенные теги.
3. В контекстном меню выбранного устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Теги**.

   Отобразится список тегов, назначенных выбранному устройству, а также способ назначения тега: вручную или по правилу.
5. При необходимости выполните одно из следующих действий:
   - Чтобы перейти к настройке правил назначения тегов, перейдите по ссылке **Настроить правила автоматического назначения тегов** (только для устройств с операционной системой Windows).
   - Чтобы переименовать тег, выделите тег и нажмите на кнопку **Переименовать**.
   - Чтобы удалить тег, выделите тег и нажмите на кнопку **Удалить**.
   - Чтобы добавить тег вручную, введите тег в поле в нижней части раздела **Теги** и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **Применить**, если вы делали изменения в разделе **Теги**, чтобы ваши изменения вступили в силу.
7. Нажмите на кнопку **ОК**.

Если вы удалили или переименовали тег в свойствах устройства, это изменение не распространится на правила назначения тегов, заданные в свойствах Сервера администрирования. Изменение будет применено только к тому устройству, в свойства которого вы внесли изменение.

Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки системной информации и параметров программы;
- загрузки журналов событий;
- создание файла дампа для программы;
- запуска диагностики и загрузки результатов диагностики;
- запуска и остановки программ.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского

устройства, для устранения неполадок самостоятельно. Также специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

В этом разделе

Подключение утилиты удаленной диагностики к клиентскому устройству

► *Чтобы подключить утилиту удаленной диагностики к клиентскому устройству, выполните следующие действия:*

1. В дереве консоли выберите любую группу администрирования.
2. В рабочей области на закладке **Устройства** в контекстном меню любого устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

   В результате открывается главное окно утилиты удаленной диагностики.
3. В первом поле главного окна утилиты удаленной диагностики определите, какими средствами требуется подключиться к устройству:
   - **Доступ средствами сети Microsoft Windows**.
   - **Доступ средствами Сервера администрирования**.
4. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами сети Microsoft Windows**, выполните следующие действия:
   - В поле **Устройство** укажите адрес устройства, к которому требуется подключиться.

     В качестве адреса устройства можно использовать IP-адрес, NetBIOS- или DNS-имя.

     По умолчанию указан адрес устройства, из контекстного меню которого запущена утилита.
   - Укажите учетную запись для подключения к устройству:
     - **Подключиться от имени текущего пользователя** (выбрано по умолчанию). Подключение

под учетной записью текущего пользователя.

- **При подключении использовать предоставленное имя пользователя и пароль**. Подключение под указанной учетной записью. Укажите **Имя пользователя** и **Пароль** нужной учетной записи.

> Подключение к устройству возможно только под учетной записью локального администратора устройства.

5. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами Сервера администрирования**, выполните следующие действия:

   - В поле **Сервер администрирования** укажите адрес Сервера администрирования, с которого следует подключиться к устройству.

     В качестве адреса Сервера можно использовать IP-адрес, NetBIOS- или DNS-имя.

     По умолчанию указан адрес Сервера, с которого запущена утилита.

   - Если требуется, установите флажки **Использовать SSL**, **Сжимать трафик** и **Устройство принадлежит подчиненному Серверу администрирования**.

     Если установлен флажок **Устройство принадлежит подчиненному Серверу администрирования**, в поле **Подчиненный Сервер администрирования** вы можете выбрать подчиненный Сервер администрирования, под управлением которого находится устройство, нажав на кнопку **Обзор**.

6. Для подключения к устройству нажмите на кнопку **Войти**.

В результате откроется окно удаленной диагностики устройства (см. рис. ниже). В левой части окна расположены ссылки для выполнения операций по диагностике устройства. В правой части окна расположено дерево объектов устройства, с которыми может работать утилита. В нижней части окна отображается процесс выполнения операций утилиты.

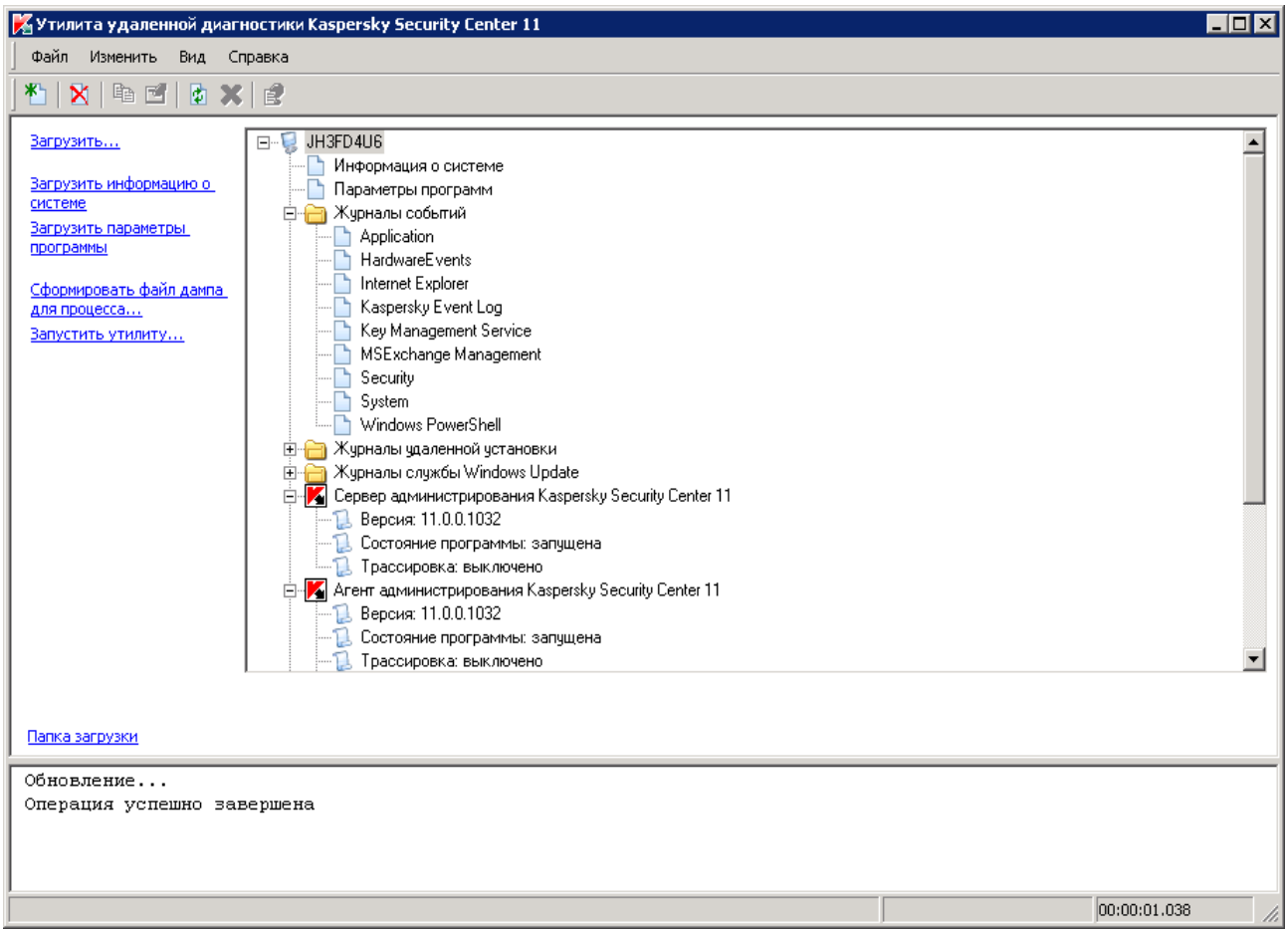


Рисунок 5: Утилита удаленной диагностики. Окно удаленной диагностики клиентского компьютера

Утилита удаленной диагностики сохраняет загруженные с устройств файлы на рабочем столе устройства, с которого она запущена.

Включение и выключение трассировки, загрузка файла трассировки

► *Чтобы включить трассировку на удаленном устройстве, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" на стр. 609.
2. В дереве объектов устройства выберите программу, для которой требуется включить трассировку.

Включение и выключение трассировки у программ с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

Если вы хотите включить трассировку для Агента администрирования, вы также можете сделать это при создании задачи Установка требуемых обновлений и закрытие уязвимостей (см. раздел "Закрытие уязвимостей в программах" на стр. 409). В этом случае Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики.

3. Чтобы включить трассировку, выполните следующие действия:

   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Выбор уровня трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

      - **Уровень трассировки**

Уровень трассировки определяет состав информации, которую содержит файл трассировки.

      - **Трассировка на основе ротации** (доступно только для Kaspersky Endpoint Security)

Программа перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

   a. Нажмите на кнопку **ОК**.

1. Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

   Чтобы включить трассировку xperf, выполните следующие действия:

   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку Xperf**.

   b. В открывшемся окне **Выбор уровня трассировки**, в зависимости от запроса специалиста Службы технической поддержки, выберите один из следующих уровней трассировки:

      - **Легкий уровень**

Файл трассировки этого типа содержит минимальный объем информации о системе.

По умолчанию выбран этот вариант.

      - **Детальный уровень**

Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных

процессов и программ, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

a. Выберите один из уровней трассировки:

- **Базовый тип**

Программа получает данные трассировки во время работы программы Kaspersky Endpoint Security.

По умолчанию выбран этот вариант.

- **Тип перезагрузки**

Программа получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

a. Также вам могут предложить включить параметр **Трассировка на основе ротации**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

b. Нажмите на кнопку **ОК**.

В некоторых случаях для включения трассировки программы безопасности требуется перезапустить эту программу и ее задачу.

Утилита удаленной диагностики позволяет получать трассировку для выбранной программы.

► *Чтобы загрузить файл трассировки программы, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В узле программы в папке **Файлы трассировки** выберите требуемый файл.
3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить файл**.

   Для файлов большого объема есть возможность загрузить только последние части трассировки.

   Вы можете удалить выделенный файл трассировки. Удаление файла возможно после выключения трассировки.

Выбранный файл загружается в местоположение, указанное в нижней части окна.

► *Чтобы выключить трассировку на удаленном устройстве, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В дереве объектов устройства выберите программу, для которой требуется выключить трассировку.

Включение и выключение трассировки у программ с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Выключить трассировку**.

Утилита удаленной диагностики выключит трассировку для выбранной программы.

Загрузка параметров программ

► *Чтобы загрузить с удаленного устройства параметры программ, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В дереве объектов окна утилиты удаленной диагностики выберите верхний узел с именем устройства.
3. В левой части окна утилиты удаленной диагностики выберите требуемое действие из следующих параметров:
   - **Загрузить информацию о системе.**
   - **Загрузить параметры программы.**
   - **Сформировать файл дампа для процесса.**

     В окне, открывшемся по этой ссылке, укажите исполняемый файл программы, для которого нужно сформировать файл дампа.
   - **Запустить утилиту.**

     В окне, открывшемся по этой ссылке, укажите исполняемый файл утилиты, которую вы хотите запустить, и параметры ее запуска.

В результате выбранная утилита будет загружена на устройство и запущена на нем.

Загрузка журналов событий

► *Чтобы загрузить с удаленного устройства журнал событий, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В папке **Журнал событий** в дереве объектов устройства выберите соответствующий журнал событий.
3. Чтобы загрузить журнал событий, перейдите по ссылке **Загрузить журнал событий <Имя журнала событий>** в левой части окна утилиты удаленной диагностики.

Выбранный журнал событий загружается в местоположение, указанное в нижней части окна.

Загрузка нескольких диагностических информационных элементов

Утилита удаленной диагностики Kaspersky Security Center позволяет загружать несколько элементов диагностической информации, включая журналы событий, системную информацию, файлы трассировки и файлы дампа.

► *Чтобы загрузить с удаленного устройства диагностическую информацию, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить**.
3. Установите флажки напротив объектов, которые вы хотите загрузить.
4. Нажмите на кнопку **Запустить**.

Каждый выбранный объект загружается в месторасположение, указанное в нижней панели.

Запуск диагностики и загрузка ее результатов

► *Чтобы запустить диагностику программы на удаленном устройстве и загрузить ее результаты, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству" (на стр. 609).
2. В дереве объектов устройства выберите необходимую программу.
3. Чтобы запустить диагностику, перейдите по ссылке **Выполнить диагностику** в левой части окна утилиты удаленной диагностики.

   В результате в узле выбранной программы в дереве объектов появится отчет диагностики.
4. Выберите сформированный отчет диагностики в дереве объектов и скачайте его по ссылке **Загрузить файл**.

Выбранный отчет загружается в местоположение, указанное в нижней части окна.

Запуск, остановка и перезапуск программ

Запуск, остановка и перезапуск программ возможны только при подключении к устройству средствами Сервера администрирования.

► *Чтобы запустить, остановить или перезапустить программу, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе"Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 609)".

2. В дереве объектов устройства выберите необходимую программу.
3. Выберите действие в левой части окна утилиты удаленной диагностики:
   - **Остановить программу.**
   - **Перезапустить программу.**
   - **Запустить программу.**

В зависимости от выбранного вами действия программа запустится, остановится или перезапустится.

Устройства с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство с программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы защиты. Kaspersky Security Center поддерживает управление такими устройствами.

► *Чтобы изменить параметры подключения устройств с защитой на уровне UEFI, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Параметры подключения к Серверу** → **Дополнительные порты**.
4. В разделе **Дополнительные порты** измените необходимые вам параметры:
   - **Открыть порт для устройств с защитой на уровне UEFI**

     Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

   - **Порт для устройств с защитой на уровне UEFI**

     Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию установлен порт 13294.
5. Нажмите на кнопку **ОК**.

Параметры управляемого устройства

Общие

Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

- **Имя**

  В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

- **Описание**

  В поле можно ввести дополнительное описание клиентского устройства.

- **Windows-домен**

  Windows-домен или рабочая группа, в которую входит устройство.

- **NetBIOS-имя**

  Имя клиентского устройства в сети Windows.

- **DNS-имя**

  Имя DNS-домена устройства.

- **IP-адрес**

  IP-адрес устройства.

- **Группа**

  Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление**

  Дата последнего обновления баз или программ на устройстве.

- **Видим в сети**

  Дата и время, когда устройство последний раз было видимо в сети.

- **Соединение с Сервером**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

  Если флажок установлен, поддерживается непрерывное соединение между Сервером администрирования и клиентским устройством.

  Если флажок снят, клиентское устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  По умолчанию флажок установлен, если на устройстве установлен Сервер

администрирования.

Если на устройстве установлен только Агент администрирования, по умолчанию флажок снят.

Защита

В разделе **Защита** представлена информация о состоянии антивирусной защиты на клиентском устройстве:

- **Статус устройства**

  Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.

- **Статус постоянной защиты**

  Статус текущего состояния постоянной защиты (см. раздел "Список управляемых устройств. Значение граф" на стр. 858) на клиентских устройствах.

  После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.

- **Последняя проверка по требованию**

  Дата и время последней антивирусной проверки на клиентском устройстве.

- **Обнаружено вирусов**

  Общее количество обнаруженных на клиентском устройстве угроз с момента установки программы безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- **Необработанных файлов**

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

Программы

В разделе **Программы** отображается список программ "Лаборатории Касперского", установленных на клиентском устройстве.

- **События**

  При нажатии на кнопку можно просмотреть список событий, произошедших на клиентском устройстве при работе программы, а также результаты выполнения задач для этой программы.

- **Статистика**

  При нажатии на кнопку можно просмотреть текущую статистическую информацию о работе программы.

- **Свойства**

  При нажатии на кнопку можно получить информацию о программе и выполнить настройку программы.

Задачи

В разделе **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. В случае отсутствия связи статус не отображается.

События

В разделе **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Теги

В разделе **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые и переименовывать старые теги, удалять теги.

Информация о системе

В разделе **Общая информация о системе** представлена информация о программе, установленной на клиентском устройстве.

Реестр программ

В разделе **Реестр программ** можно просмотреть реестр установленных на клиентском устройстве программ и обновлений для них, а также настроить отображение реестра программ.

Информация об установленных программах предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**. Информация об установленных программах доступна только для устройств под управлением Windows.

Агент администрирования предоставляет информацию о программах на основе данных системного реестра.

- **Показывать только несовместимые программы безопасности**

  Если флажок установлен, в списке программ отображаются только те программы безопасности, которые несовместимы с программами "Лаборатории Касперского".

  По умолчанию флажок снят.

- **Показывать обновления**

Если флажок установлен, в списке программ отображаются не только программы, но и установленные для них пакеты обновлений.

По умолчанию флажок снят.

- **Экспортировать в файл**

  Нажмите эту кнопку, чтобы экспортировать список программ, установленных на устройстве, в файл формата CSV или TXT.

- **История**

  Нажмите эту кнопку, чтобы просмотреть события, относящиеся к установке программ на устройство. Отобразится следующая информация:

  - дата и время, когда программа была установлена на устройство;
  - название программы;
  - версия программы.

- **Свойства**

  Нажмите эту кнопку, чтобы просмотреть свойства программы, выбранной в списке программ, установленных на устройстве. Отобразится следующая информация:

  - название программы;
  - версия программы;
  - поставщик программы.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

Реестр оборудования

В разделе **Реестр оборудования** можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

Сеансы

В разделе **Сеансы** представлена информация о владельце клиентского устройства, а также об учетных записях пользователей, которые работали с выбранным клиентским устройством.

Информация о доменных пользователях формируется на основе данных Active Directory. Информация о локальных пользователях предоставляется Диспетчером учетных записей безопасности (Security Account Manager), установленным на клиентском устройстве.

- **Владелец устройства**

В поле **Владелец устройства** отображается имя пользователя, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с клиентским устройством.

По кнопкам **Назначить** и **Свойства** можно выбрать владельца устройства и просмотреть информацию о пользователе, назначенном владельцем устройства.

По кнопке с красным крестом можно удалить текущего владельца устройства.

В списке содержатся учетные записи пользователей, которые работают с клиентским устройством.

- **Имя**

  Имя устройства в Windows-сети.

- **Имя участника**

  Имя пользователя (доменное или локальное), который выполнил вход в систему на этом устройстве.

- **Учетная запись**

  Учетная запись пользователя, который выполнил вход в систему на этом устройстве.

- **Электронная почта**

  Адреса электронной почты пользователя.

- **Телефон**

  Номер телефона пользователя.

  Инциденты

  В разделе **Инциденты** можно просматривать, редактировать и создавать инциденты для клиентского устройства. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные программы с личного съемного диска, администратор может создать по этому поводу инцидент. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте инцидента, и может добавить ссылку на пользователя или пользователей.

  Инцидент, для которого выполнены необходимые действия, называется *обработанным*. Наличие необработанных инцидентов может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список инцидентов, созданных для устройства. Инциденты классифицируются по уровню важности и типу. Тип инцидента определяется программой "Лаборатории Касперского", которая создает инцидент. Обработанные инциденты можно отметить в списке, установив флажок в графе **Обработан**.

Уязвимости в программах

В разделе **Уязвимости в программах** можно просмотреть список с информацией об уязвимостях сторонних программ, установленных на клиентских устройствах. С помощью строки поиска над списком вы можете

искать в списке уязвимости по имени уязвимости.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список уязвимостей в файле. По умолчанию программа экспортирует список уязвимостей в файл формата CSV.

- **Показывать только те уязвимости, которые можно закрыть**

  Если флажок установлен, в разделе отображаются уязвимости, которые можно закрыть патчем.

  Если флажок снят, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

  По умолчанию флажок установлен.

Неустановленные обновления

В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Показывать установленные обновления**

  Если флажок установлен, в списке обновлений отображаются и не установленные обновления, и обновления, которые уже установлены на клиентском устройстве.

  По умолчанию флажок снят.

Действующие профили политик

- **Список профилей политик**

  В списке можно просмотреть информацию о действующих профилях политики, которые активны на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке действующие профили политик по имени политики или по имени профиля политики.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список активных профилей политики в файле. По умолчанию программа экспортирует список профилей политики в файл формата CSV.

Агенты обновлений

В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию программа экспортирует список устройств в файл формата CSV.

  По кнопке **Свойства** вы можете посмотреть и настроить параметры точки

распространения, с которым взаимодействует устройство.

См. также

Настройка общих параметров Сервера администрирования 556

Общие параметры политик

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Политика для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.
  - **Неактивная политика**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры из политики верхнего уровня**

    Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию флажок установлен.
  - **Форсировать наследование параметров дочерними политиками**

    Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры родительской политики**.

    Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие**

Закладка **Критическое событие** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

На каждой закладке отображается список типов событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений (см. раздел "Настройка параметров уведомлений о событиях" на стр. 231), указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Для выбора нескольких типов событий используйте клавиши Shift или Ctrl, для выбора всех типов используйте кнопку **Выбрать все**.

См. также:

Контроль возникновения вирусных эпидемий 559

Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки выберите политику Агента администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Политика для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.
  - **Неактивная политика**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры из политики верхнего уровня**

    Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию флажок установлен.
  - **Форсировать наследование параметров дочерними политиками**

    Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры родительской политики**.

    Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию флажок снят.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие**

Закладка **Критическое событие** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

На каждой закладке отображается список типов событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий (см. раздел "Настройка параметров уведомлений о событиях" на стр. 231). Однако можно изменить определенные параметры для заданных типов событий.

Для выбора нескольких типов событий используйте клавиши Shift или Ctrl, для выбора всех типов используйте кнопку **Выбрать все**.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если флажок установлен, клиентские устройства получают обновления только через точки распространения, а не напрямую с серверов обновлений.

  Если флажок снят, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, от главного Сервера администрирования, из локальной или сетевой папки.

  По умолчанию флажок снят.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Использовать пароль деинсталляции**

  Если флажок установлен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

  По умолчанию флажок снят.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, параметры недоступны для изменения. Параметры раздела **Хранилища** доступны только для устройств под управлением Windows:

- **Информация об установленных программах**

  Если флажок установлен, на Сервер администрирования отправляется информация

о программах, установленных на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация об обновлениях Центра обновления Windows**

  Если флажок установлен, на Сервер администрирования отправляется информация об обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

  По умолчанию флажок установлен.

- **Информация об уязвимостях программного обеспечения**

  Если флажок установлен, на Сервер администрирования отправляется информация об уязвимостях программного обеспечения, обнаруженных на клиентских устройствах.

  По умолчанию флажок установлен.

- **Информация о реестре оборудования**

Если флажок установлен, на Сервер администрирования отправляется информация об оборудовании, найденном в процессе обнаружения устройств.

По умолчанию флажок установлен.

Обновления и уязвимости в программах

В разделе **Обновления и уязвимости в программах** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей: Параметры раздела **Обновления и уязвимости в программах** доступны только для устройств под управлением Windows:

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Если флажок установлен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

  Если флажок снят, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

  По умолчанию флажок снят.

- С помощью параметра **Разрешить пользователям управлять установкой обновлений Центра обновления Windows** вы можете ограничить обновления Windows, которые пользователи могут устанавливать на своих устройствах вручную, с помощью Центра обновления Windows.

Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, новый параметр, который вы выбрали **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

Выберите параметр из раскрывающегося списка:

- **Устанавливать все применимые обновления Центра обновления Windows**

  Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

  Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

  Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

  Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

  Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- В блоке параметров **Режим поиска обновлений Windows Update** можно выбрать режим поиска обновлений:
  - **Активна.**

    Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

    По умолчанию выбран этот вариант.
  - **Пассивный**

    Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.
  - **Выключен**

    Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.
- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

  Если флажок установлен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

  По умолчанию флажок установлен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления программы требуется перезагрузка операционной системы: Параметры раздела **Управление перезагрузкой** доступны только для устройств под управлением Windows:

- **Не перезагружать операционную систему**

  Перезагрузка операционной системы не выполняется.

- **При необходимости перезагрузить операционную систему автоматически**

  При необходимости перезагрузка операционной системы выполняется автоматически.
- **Спросить у пользователя**

  Программа запрашивает у пользователя разрешение перезагрузить операционную систему.

  По умолчанию этот вариант выбран.

- **Периодичность напоминания о необходимости установки (мин)**

  Если флажок установлен, программа запрашивает у пользователя разрешение на перезагрузку операционной системы с периодичностью, указанной в поле рядом с флажком. По умолчанию периодичность повторных запросов составляет 5 минут.

  Если флажок снят, программа не запрашивает разрешение на перезагрузку повторно.

  По умолчанию флажок установлен.

- **Принудительно перезагружать через (мин)**

  Если флажок установлен, после запроса у пользователя операционная система перезагружается принудительно по истечении времени, указанного в поле рядом с флажком.

  Если флажок снят, принудительная перезагрузка не выполняется.

По умолчанию флажок установлен.

- **Принудительно закрывать программы в заблокированных сессиях через (мин)**

  Принудительное завершение работы программ, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

Если флажок установлен, работа программ на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

Если флажок снят, работа программ на заблокированном устройстве не прекращается.

По умолчанию флажок снят.

Совместный доступ к рабочему столу Windows

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу: Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

  Если флажок установлен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

  - в журнале событий на удаленном устройстве;
  - в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
  - в базе событий Kaspersky Security Center.

  Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

Если флажок снят, аудит действий администратора на удаленном устройстве выключен.

По умолчанию флажок снят.

- **Маски файлов, чтение которых нужно отслеживать**

  В списке содержатся маски файлов. Когда аудит включен, программа отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

  В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, программа отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Автоматическая установка патчей со статусом *Не определено* доступна для версий Kaspersky Security Center Service Pack 2 и выше.

  Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  По умолчанию параметр включен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее**

(рекомендуется)

Если флажок снят, офлайн-модель получения обновлений выключена. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых программ. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для программ на клиентских устройствах, но подключение не требуется для обновления.

Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

По умолчанию параметр включен.

подключения;

Раздел **Подключения** включает три вложенных раздела:

- **Сеть.**
- **Профили соединений** (только для Windows).
- **Расписание соединений.**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Сжимать сетевой трафик**

    Если флажок установлен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

Если флажок установлен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

По умолчанию флажок установлен.

- **Использовать SSL-соединение**

  Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию флажок установлен.

- **Использовать шлюз соединений точки распространения (при наличии) в параметрах подключения по умолчанию**

  Если флажок установлен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

  По умолчанию флажок установлен.

- **Использовать UDP-порт**

  Если флажок установлен, соединение клиентского устройства с Сервером администрирования будет устанавливаться через UDP-порт.

  По умолчанию флажок установлен.

- **Номер UDP-порта**

В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

Используется десятичная форма записи.

Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный межсетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

В разделе **Профили соединений** можно задать параметры сетевого местоположения, настроить профили подключения к Серверу администрирования, включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows:

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного Сервера

администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

Профили подключения поддерживаются только для устройств под управлением Windows.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если флажок установлен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. 577). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

  Если флажок снят, программы будут использовать активные политики.

  По умолчанию флажок снят.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию этот вариант выбран.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Точки распространения

Раздел **Точки распространения** включает четыре подраздела:

- **Обнаружение устройств.**
- **Параметры подключения к интернету.**

- **Прокси-сервер KSN.**
- **Обновления.**

В подразделе **Обнаружение устройств** вы можете настроить автоматический опрос сети. Параметры опроса сети доступны только для устройств под управлением Windows.

- В блоке **Обнаружение устройств** можно включить автоматический опрос сети и настроить периодичность опроса:
  - **Разрешить опрос сети**

    Если флажок установлен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить период быстрого опроса** и **Настроить период полного опроса**.

    Если флажок снят, Сервер администрирования не выполняет опрос сети.

    Период обнаружения устройств для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период опроса Windows-доменов (мин)** и **Период опроса сети (мин)**. Поля доступны, если флажок установлен.

    По умолчанию флажок установлен.
- В блоке **Опрос IP-диапазонов** можно включить автоматический опрос IP-диапазонов и настроить периодичность опроса:
  - **Разрешить опрос IP-диапазонов**

    Если флажок установлен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить параметры опроса**.

    Если флажок снят, Сервер администрирования не выполняет опрос IP-диапазонов.

    Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

    По умолчанию флажок снят.
- В блоке параметров **Опрос Active Directory** можно включить автоматическое обнаружение устройств в соответствии со структурой Active Directory и настроить его периодичность:
  - **Разрешить опрос Active Directory**

    Если флажок установлен, Сервер администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

    Если флажок снят, Сервер администрирования не выполняет опрос Active Directory.

    Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок установлен.

В разделе **Параметры подключения к интернету** можно настроить параметры доступа в интернет:

- **Использовать прокси-сервер**

  Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

  По умолчанию флажок снят.

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если флажок установлен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию флажок снят.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

В разделе **Прокси-сервер KSN** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования**

как прокси-сервер и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. 736) .

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Переслать KSN запрос Серверу администрирования**

Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

По умолчанию параметр включен.

- **Доступ к облачной-службе KSN непосредственно через интернет**

Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN.

- **TCP-порт**

Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию флажок снят, подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

В подразделе **Обновления** вы можете настроить, будет ли Агент администрирования загружать фалы различий:

- **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. раздел "Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"" на стр. 361).

По умолчанию параметр включен.

История ревизий

В разделе **История ревизий** можно посмотреть историю ревизий Агента администрирования (см. раздел "Работа с ревизиями объектов" на стр. 654). Вы можете сравнивать ревизии, просматривать ревизии и выполнять другие операции, такие как сохранять ревизии в файл, откатывать ревизии, добавлять и изменять описания ревизий.

Параметры политики Агента администрирования, которые доступны для разных операционных систем, приведены в таблице ниже.

Таблица 59. Параметры политики Агента администрирования

Раздел Политики	Windows.	Mac	Linux
Общие	+	+	+

Раздел Политики	Windows.	Mac	Linux
Настройка событий	+	+	+
Параметры	+	+ * кроме флажка **Использовать пароль деинсталляции**	+ * кроме флажка **Использовать пароль деинсталляции**
Хранилища	+	Нет	Нет
Обновления и уязвимости в программах	+	Нет	Нет
Управление перезагрузкой	+	Нет	Нет
Совместный доступ к рабочему столу Windows	+	Нет	Нет
Управление патчами и обновлениями	+	Нет	Нет
Сеть → Сеть	+	+ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**	+ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**
Сеть → Подключение	+	Нет	Нет
Сеть → Менеджер соединений	+	+	+
Точки распространения → Обнаружение устройств	+	Нет	Нет
Точки распространения → Параметры подключения к интернету	+	+	+
Точки распространения → Прокси-сервер KSN	+	Нет	Нет
Точки распространения → Обновления	+	Нет	Нет
История ревизий	+	+	+

Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях пользователей управляемых устройств и учетных записях внутренних пользователей Kaspersky Security Center (администраторов, управляющих устройствами пользователей). В разделе приведены инструкции по созданию учетных записей и ролей пользователей Kaspersky Security Center. Раздел также содержит инструкции по работе со списками сертификатов и мобильных устройств пользователя, по рассылке сообщений пользователям.

В этом разделе

Работа с учетными записями пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записей этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. раздел "Работа с внутренними пользователями" на стр. 561). Учетные записи внутренних пользователей создаются (см. раздел "Добавление учетной записи внутреннего пользователя" на стр. 640) и используются только внутри Kaspersky Security Center.

Все учетные записи пользователей можно просмотреть в папке **Учетные записи пользователей** в дереве

консоли. Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

Вы можете выполнять с учетными записями пользователей и группами учетных записей следующие действия:

- настраивать права доступа пользователей к функциям программы с помощью ролей (см. раздел "Настройка прав.Роли пользователей" на стр. 646);
- рассылать сообщения пользователям с помощью электронной почты и SMS (см. раздел "Рассылка сообщений пользователям" на стр. 652);
- просматривать список мобильных устройств пользователя (см. раздел "Просмотр списка мобильных устройств пользователя" на стр. 653);
- выписывать и устанавливать сертификаты на мобильные устройства пользователя (см. раздел "Установка сертификата пользователю" на стр. 653);
- просматривать список сертификатов, выписанных пользователю (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. 654).

Добавление учетной записи внутреннего пользователя

► *Чтобы добавить новую учетную запись пользователя Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В рабочей области нажмите на кнопку **Добавить пользователя**.
3. В открывшемся окне **Новый пользователь** укажите параметры нового пользователя:
   -  (Имя пользователя).

     Пожалуйста, будьте внимательны при вводе имени пользователя. Вы не сможете его изменить после сохранения изменений.
   - **Описание.**
   - **Полное имя.**
   - **Основная электронная почта.**
   - **Основной номер телефона.**
   - **Пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 16 символов.

- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A-Z);
  - нижний регистр (A-Z) (a-z);
  - числа (0-9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", расположенных рядом друг с другом.

Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля" (см. раздел "Изменение количества попыток ввода пароля" на стр. 643).
Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок  заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись, если вы хотите создать учетную запись заранее, но активировать ее позже.

4. Нажмите на кнопку **ОК**.

Созданная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение учетной записи внутреннего пользователя

► *Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области дважды щелкните учетную запись внутреннего пользователя, которую требуется изменить.
3. В открывшемся окне **Свойства: <имя пользователя>** измените параметры учетной записи пользователя:

- **Описание.**
- **Полное имя.**
- **Основная электронная почта.**
- **Основной номер телефона.**
- **Пароль** для подключения пользователя к Kaspersky Security Center.

  Пароль должен соответствовать следующим правилам:

  - Длина пароля должна быть от 8 до 16 символов.
  - Пароль должен содержать символы как минимум трех групп списка ниже:
    - верхний регистр (A-Z);
    - нижний регистр (A-Z) (a-z);
    - числа (0-9);
    - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
  - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", расположенных рядом друг с другом.

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  > Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля" (см. раздел "Изменение количества попыток ввода пароля" на стр. 643).
  > Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок  заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.

4. Нажмите на кнопку **ОК**.

Измененная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Изменение количества попыток ввода пароля

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля, следуя инструкции ниже.

► *Чтобы изменить количество попыток ввода пароля, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите к следующему разделу:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Если параметр SrvSplPpcLogonAttempts отсутствует в разделе реестра, создайте его. Тип значения параметра – DWORD.

   Этот параметр не создается по умолчанию при установке Kaspersky Security Center.
4. Укажите требуемое количество попыток в качестве значения параметра SrvSplPpcLogonAttempts.
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
6. Перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

Настройка проверки уникальности имени внутреннего пользователя

Вы можете настроить проверку уникальности имени внутреннего пользователя Kaspersky Security Center при его добавлении в программу. Проверка на уникальность имени внутреннего пользователя может выполняться только на виртуальном Сервере или главном Сервере, для которого создается учетная запись пользователя, или на всех виртуальных Серверах и главном Сервере. По умолчанию проверка на уникальность имени внутреннего пользователя выполняется на всех виртуальных Серверах и на главном Сервере администрирования.

► *Чтобы включить проверку уникальности имени внутреннего пользователя в рамках виртуального Сервера или главного Севера, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:

- для 64-разрядной системы:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM

- для 32-разрядной системы:

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000001.

   По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена только на том виртуальном Сервере, на котором был создан внутренний пользователь, или на главном Сервере, если пользователь был создан на главном Сервере.

► *Чтобы включить проверку уникальности имени внутреннего пользователя на всех виртуальных Серверах и главном Сервере, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:

   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM

   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена на всех виртуальных Серверах и на главном Сервере администрирования.

Добавление группы безопасности

Вы можете добавлять группы безопасности (группы пользователей), гибко настраивать состав групп и доступ группы безопасности к разным функциям программы. Группам безопасности можно давать названия, соответствующие их назначению. Например, название может соответствовать расположению пользователей в офисе или названию структурного подразделения компании, к которому относятся пользователи.

Один пользователь может входить в состав нескольких групп безопасности. Учетная запись пользователя под управлением виртуального Сервера администрирования может входить только в группы безопасности

этого виртуального Сервера и иметь права доступа только в рамках этого виртуального Сервера.

► *Чтобы добавить группу безопасности, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Добавить группу безопасности**.

   Откроется окно **Добавить группу безопасности**.

3. В окне **Добавить группу безопасности** в разделе **Общие** укажите имя группы.

   Имя группы не может превышать 255 символов и не может содержать символы *, <, >, ?, \, :, |. Имя группы должно быть уникальным.

   Вы можете ввести описание группы в поле ввода **Описание**. Заполнение поля **Описание** не является обязательным.

4. Нажмите на кнопку **ОК**.

Добавленная группа безопасности отобразится в папке **Учетные записи пользователей** в дереве консоли. Вы можете добавить пользователей в созданную группу (см. раздел "Добавление пользователя в группу" на стр. 645).

Добавление пользователя в группу

► *Чтобы добавить пользователя в группу, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В списке учетных записей пользователей и групп выберите группу, в которую нужно добавить пользователя.

3. В окне свойств группы выберите раздел **Пользователи группы**, затем нажмите на кнопку **Добавить**.

   В результате откроется окно со списком пользователей.

4. В списке выберите пользователя или пользователей, которых нужно включить в состав группы.

5. Нажмите на кнопку **ОК**.

Пользователь добавлен в группу и отображается в списке пользователей группы.

Настройка прав. Роли пользователей

Вы можете гибко настраивать доступ администраторов, пользователей и групп пользователей к разным функциям программы. Предоставлять пользователям права доступа к функциям программы можно двумя способами:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Роль пользователя – это заранее созданный и настроенный набор прав доступа к функциям программы. Роль можно предоставить пользователю или группе пользователей. Применение ролей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к программе. Права доступа в роли настраивают в соответствии с "типовыми" задачами и служебными обязанностями пользователей. Например, роль пользователя может иметь права только на чтение и отправление информационных команд на мобильные устройства других пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В программе можно создавать неограниченное количество ролей.

Вы можете настроить доступ к различным функциям программы для следующих объектов:

- Серверы администрирования;
- группы администрирования;
- Виртуальные Серверы администрирования

В этом разделе

Добавление роли пользователя

► *Чтобы добавить роль пользователя, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойства Сервера администрирования перейдите в раздел **Роли пользователей** и нажмите на кнопку **Добавить**.

4. В окне **Новая роль** настройте параметры роли:
   - Выберите раздел **Общие** и укажите имя роли.

     Имя роли не может превышать 100 символов.
   - В разделе **Права** настройте набор прав, установив флажки **Разрешить** и **Запретить** напротив функций программы.

   Если вы работаете на главном Сервере администрирования, вы можете включить параметр **Передать список ролей подчиненному Серверу администрирования**, чтобы распространять роли пользователей на подчиненные Серверы (см. раздел "Распространение пользовательских ролей на подчиненные Серверы администрирования" на стр. 650).
5. Нажмите на кнопку **ОК**.

В результате роль будет сохранена.

Роли пользователей, созданные для Сервера администрирования, отображаются в окне свойств Сервера в разделе **Роли пользователей**. Вы можете изменять и удалять роли пользователей, а также назначать роли группам пользователей или отдельным пользователям (см. раздел "Назначение роли пользователю или группе пользователей" на стр. 647).

Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. 556).

Назначение роли пользователю или группе пользователей

► *Чтобы назначить роль пользователю или группе пользователей, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которой нужно присвоить роль.

   Если пользователь или группа отсутствует в поле, добавьте их по кнопке **Добавить**.

   При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей.
5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.
6. В окне **Роли пользователей** выберите роль для группы пользователей.
7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** доступен, если в окне настройки интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам пользователей, чтобы использовать различные возможности Сервера администрирования и программ "Лаборатории Касперского", для которых у вас есть плагины управления, например, Kaspersky Endpoint Security для Windows.

► *Чтобы назначить права пользователю или группе пользователей, выполните следующие действия:*

1. В дереве консоли выполните одно из следующих действий:
   - Раскройте узел **Сервер администрирования** и выберите подпапку с именем требуемого Сервера администрирования.
   - Выберите группу администрирования.
2. В контекстном меню Сервера администрирования или группы администрирования выберите пункт **Свойства**.
3. В открывшемся окне **свойств** Сервера администрирования (или окне свойств групп администрирования) выберите раздел **Безопасность**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. 556).
4. В разделе **Безопасность** в списке **Имена групп или пользователей** выберите пользователя или группу пользователей.
5. В списке прав в нижней части окна, на закладке **Права** настройте права для пользователей или групп:
   a. Нажмите на значок плюс (+), чтобы раскрыть узел в списке, и назначьте права.
   b. Установите флажки **Разрешить** и **Запретить** рядом с требуемыми правами.

      Пример 1: Раскройте узел **Доступ к объектам независимо от их списков ACL** или узел **Удаленные объекты**, и выберите **Чтение**.

      Пример 2: Раскройте узел **Базовая функциональность** и выберите **Изменение**.
6. После того как вы настроили набор прав, нажмите на кнопку **Применить**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
  - управление группами администрирования (только для Kaspersky Security Center 11 и выше);
  - доступ к объектам независимо от их списков ACL (только для Kaspersky Security Center 11 и выше);
  - базовая функциональность;
  - удаленные объекты (только для Kaspersky Security Center 11 и выше);
  - обработка событий;
  - операции с Сервером администрирования (только в окне свойств Сервера администрирования);
  - развертывание программ "Лаборатории Касперского";
  - ключи;
  - управление отчетами (только для Kaspersky Security Center 11 и выше);
  - иерархия Серверов;
  - права пользователей;
  - Виртуальные Серверы администрирования
- Управление мобильными устройствами
  - Общие
- Управление системой
  - подключения;
  - Инвентаризация оборудования
  - управление доступом в сеть;
  - развертывание операционной системы;
  - управление уязвимостями и патчами;
  - Удаленная установка
  - инвентаризация программ.

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;

- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Роли для определенных должностей

Роли – это наборы прав, которые вы можете назначить пользователям Kaspersky Security Center. Следующие роли могут быть связаны с определенными должностями:

Таблица 60. Роли для определенных должностей

Роль	Комментарий
Аудитор	Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права **Чтение** и **Изменение** для области **Удаленные объекты**). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Только просмотр	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль сотруднику безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Офицер безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

Эти роли присутствуют в Kaspersky Security Center, начиная с версии 11.

Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить программы для автоматического распространения ролей

пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

► *Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выполните одно из следующих действий:
   - В дереве консоли в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
   - Если у вас есть активная политика Сервера администрирования, в рабочей области папки **Политики** в контекстном меню этой политики выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования или в окне свойств политики перейдите в раздел **Роли пользователей**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел "**Настройка общих параметров Сервера администрирования**" на стр. 556).

4. Включите параметр **Передать список ролей подчиненному Серверу администрирования**.
5. Нажмите на кнопку **ОК**.

   Программа копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью значка замок ( ). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~~1, ~~2 (номер может быть случайным).

Если отключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования

становятся независимыми, их можно изменять или удалять.

Назначение пользователя владельцем устройства

Вы можете назначить пользователя владельцем устройства, чтобы "закрепить" устройство за этим пользователем. При необходимости выполнить какие-либо действия с устройством (например, обновить аппаратное обеспечение) администратор может проинформировать владельца устройства и согласовать действия с ним.

► *Чтобы назначить пользователя владельцем устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки на закладке **Устройства** выберите устройство, для которого нужно назначить владельца.
3. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Информация о системе** → **Сеансы**.
5. Нажмите на кнопку **Назначить** рядом с полем **Владелец устройства**.
6. В окне **Пользовательская выборка** выберите пользователя, которого нужно назначить владельцем устройства и нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК**.

В результате владелец устройства будет назначен. По умолчанию поле **Владелец устройства** заполнено значением из Active Directory и обновляется при каждом опросе Active Directory (см. раздел "Опрос Active Directory" на стр. 242). Вы можете просмотреть список владельцев устройств в отчете **Отчет о владельцах устройств**. Отчет можно создать с помощью мастера создания отчетов (см. раздел "Создание шаблона отчета" на стр. 463).

Рассылка сообщений пользователям

► *Чтобы отправить сообщение пользователю по электронной почте, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню пользователя выберите **Отправить сообщение по электронной почте**.
3. Заполните необходимые поля в окне **Сообщение для пользователя** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на электронную почту, указанную в свойствах пользователя.

► *Чтобы отправить SMS-сообщение пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

2. В контекстном меню пользователя выберите **Отправить SMS-сообщение**.
3. Заполните необходимые поля в окне **Текст SMS** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на мобильное устройство, номер которого указан в свойствах пользователя.

Просмотр списка мобильных устройств пользователя

► *Чтобы просмотреть список мобильных устройств пользователя, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Мобильные устройства**.

В разделе **Мобильные устройства** можно просмотреть список мобильных устройств пользователя и информацию о мобильных устройствах. По кнопке **Экспортировать в файл** можно сохранить список мобильных устройств в файле.

Установка сертификата пользователю

Вы можете установить пользователю сертификаты трех типов:

- общий сертификат, необходим для идентификации мобильного устройства пользователя;
- почтовый сертификат, необходим для настройки корпоративной почты на мобильном устройстве пользователя;
- VPN сертификат, необходим для настройки виртуальной частной сети на мобильном устройстве пользователя.

► *Чтобы выписать сертификат пользователю и установить его, выполните следующие действия:*

1. В дереве консоли откройте папку **Учетные записи пользователей** и выберите учетную запись пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера установки сертификата сертификат будет создан и установлен пользователю. Список всех установленных сертификатов пользователя можно просмотреть и экспортировать в файле (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. 654).

Просмотр списка сертификатов, выписанных пользователю

► *Чтобы просмотреть список всех сертификатов, выписанных пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Сертификаты**.

В разделе **Сертификаты** можно просмотреть список сертификатов пользователя и информацию о сертификатах. По кнопке **Экспортировать в файл** можно сохранить список сертификатов в файле.

Об администраторе виртуального Сервера

При необходимости можно создать несколько учетных записей администраторов виртуального Сервера.

Администратор виртуального Сервера администрирования является внутренним пользователем Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия.* Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- Серверы администрирования;
- Политики
- Задачи
- группы администрирования;
- учетные записи пользователей;
- Инсталляционные пакеты

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;

- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Описание**. В окне **Описание ревизии объекта** введите текст описания ревизии.

В этом разделе

О ревизиях объектов

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта (см. раздел "Сравнение ревизий объекта" на стр. 657);
- просматривать выбранную ревизию (см. раздел "Просмотр раздела История ревизий" на стр. 656);
- откатывать изменения объекта к выбранной ревизии (см. раздел "Откат изменений" на стр. 659);
- сохранять ревизии в файле формата TXT (см. раздел "Сохранение ревизии объекта в файле" на стр. 659).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта (см. раздел "Добавление описания ревизии" на стр. 661).

Просмотр раздела История ревизий

Вы можете сравнить ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► *Чтобы просмотреть раздел **История ревизий** объекта, выполните следующие действия:*

1. В дереве консоли выберите один из объектов:
   - узел **Сервер администрирования**;
   - папку **Политики**;
   - папку **Задачи**;
   - папку группы администрирования;
   - папку **Учетные записи пользователей**;
   - папку **Удаленные объекты**;
   - папку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.

2. В зависимости от местоположения соответствующего объекта выполните одно из следующих действий:

   - Если объект находится в узле **Сервер администрирования** или в папке группы администрирования, выберите пункт **Свойства** в контекстном меню объекта.
   - Если объект находится в папках **Политики**, **Задачи**, **Учетные записи пользователей**, **Удаленные объекты**, или **Инсталляционные пакеты**, выберите папку и в соответствующей рабочей области выберите объект.

   Откроется окно свойств объекта.

3. В окне свойств объекта выберите раздел **История ревизий**.

История ревизий отображается в рабочей области.

Сравнение ревизий объекта

Вы можете сравнить предыдущие ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► *Чтобы сравнить ревизии объекта, выполните следующие действия:*

1. Выберите объект и перейдите к окну свойств этого объекта.
2. В окне свойств задачи выберите раздел **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. 656).
3. В рабочей области в списке ревизий объекта выберите ревизию для сравнения.

   Для выбора более двух ревизий объекта используйте клавиши SHIFT и CTRL.

4. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите одно из значений:
     - **Сравнить с текущей ревизией**

       Выберите этот вариант, чтобы сравнить выбранную ревизию с текущей.

     - **Сравнивать выбранные ревизии**

       Выберите этот вариант, чтобы сравнить две выбранные ревизии.

     - **Сравнить с другим объектом**

       При работе с ревизиями задач выберите вариант **Сравнить с другой задачей**, чтобы сравнить выбранную ревизию с ревизией другой задачи.

       При работе с ревизиями политик выберите вариант **Сравнить с другой политикой**, чтобы сравнить выбранную ревизию с ревизией другой политики

   - Откройте окно свойств требуемой ревизии двойным щелчком мыши. В открывшемся окне свойств ревизии нажмите на одну из следующих кнопок:

- **Сравнить с текущей**

  Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с текущей.

- **Сравнить с предыдущей**

  Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с предыдущей.

Отчет о сравнении ревизий в формате HTML отображается в вашем браузере по умолчанию.

В отчете можно свернуть некоторые блоки параметров ревизии. Чтобы свернуть блок параметров ревизии, нажмите на значок рядом с названием блока.

В ревизии Сервера администрирования попадает информация об изменениях, кроме информации из следующих областей:

- раздела **Трафик**;
- раздела **Правила назначения тегов**;
- раздела **Уведомление**;
- раздела **Точки распространения**;
- раздела **Вирусная атака**.

  Из раздела **Вирусная атака** не будет записана информация о настройке активации политик по событию Вирусная атака.

Вы можете сравнивать ревизии удаленного объекта с ревизией существующего объекта, но не наоборот: вы не можете сравнивать ревизии существующего объекта с ревизией удаленного объекта.

Установка срока хранения ревизий объектов и информации об удаленных объектах

Срок хранения ревизий объекта и срок хранения информации об удаленных объектах одинаковы. Срок, заданный по умолчанию, – 90 дней. Этого достаточно для регулярного аудита программы.

Только пользователи с правами **Изменение** в области **Удаленные объекты** могут изменить срок хранения ревизий объектов и информации об удаленных объектов (см. раздел "Назначение прав пользователям и группам пользователей" на стр. 648).

► *Чтобы изменить срок хранения ревизий объектов и информации об удаленных объектах, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно изменить срок хранения ревизий объектов и информации об удаленных объектах.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Хранение истории ревизий** укажите требуемый срок хранения (в днях).
4. Нажмите на кнопку **ОК**.

Ревизии объектов и информация об удаленных объектах будут храниться указанное количество дней.

Просмотр ревизии объекта

Если вам понадобилось узнать, какие изменения проводились с объектом в определенный период, вы можете просмотреть ревизии объекта.

► *Чтобы просмотреть ревизии объекта, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. 656) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно посмотреть.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Посмотреть ревизию**.
   - Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на кнопку **Посмотреть ревизию**.

Отобразится отчет с параметрами выбранной ревизии объекта в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии объекта. Чтобы свернуть блок параметров ревизии, нажмите на значок ▲ рядом с названием блока.

Сохранение ревизии объекта в файле

Вы можете сохранить ревизию объекта в текстовом файле, например, чтобы отправить файл по электронной почте.

► *Чтобы сохранить ревизию объекта в файле, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. 656) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно сохранить.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Сохранить в файл**.

Ревизия будет сохранена в файле формата TXT.

Откат изменений

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► *Чтобы откатить изменения объекта, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. 656) объекта.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. 656) объекта.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Описание**.
4. В окне **Описание ревизии объекта** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.
5. Нажмите на кнопку **ОК**.

Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователи;
- группы пользователей;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней) (см. раздел "Установка срока хранения ревизий объектов и информации об удаленных объектах" на стр. 658). Можно изменить время хранения только при наличии права (см. раздел "Назначение прав пользователям или группам пользователей" на стр. 648) на **Изменение** для области **Удаленные объекты**.

В этом разделе

Удаление объекта

Вы можете удалять объекты, такие как политики, задачи, инсталляционные пакеты, внутренних пользователей и группы внутренних пользователей, если у вас есть права на изменение для категории Базовая функциональность (подробную информацию см. в разделе Назначение прав пользователям и группам пользователей на стр. 648).

► *Чтобы удалить объект, выполните следующие действия:*

1. В рабочей области требуемой папки дерева консоли выберите объект.
2. Выполните одно из следующих действий:
   - В контекстном меню объекта выберите пункт **Удалить**.
   - Нажмите на кнопку DELETE.

Объект будет удален, и информация об этом будет записана в базу данных.

Просмотр информации об удаленных объектах

Информация об удаленных объектах хранится в папке **Удаленные объекты** такой же срок, как и ревизии объекта (рекомендуемый срок составляет 90 дней).

Только пользователи с правами на **Чтение** для области **Удаленные объекты** могут просматривать список удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей на стр. 648).

► *Чтобы просмотреть список удаленных объектов,*

В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).

Если у вас нет прав на чтение для области **Удаленные объекты**, в папке **Удаленные объекты** будет отображаться пустой список.

В рабочей области папки **Удаленные объекты** содержится следующая информация об удаленных

объектах:

- **Название**. Название удаленного объекта.
- **Тип**. Тип объекта, такой как политика, задача или инсталляционный пакет.
- **Время**. Время, когда объект был удален.
- **Пользователь**. Учетная запись пользователя, который удалил объект.

► *Чтобы просмотреть больше информации об удаленном объекте, выполните следующие действия:*

1. В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).
2. В рабочей области папки **Удаленные объекты** выберите нужный объект.

   В правой части рабочей области отобразится поле для работы с выбранным объектом.
3. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в блоке работы с выбранным объектом.
   - В контекстном меню объекта выберите пункт **Свойства**.

   Откроется окно свойств объекта, в котором отображается следующая информация:
   - **Общие**
   - **История ревизий** (см. раздел "**Работа с ревизиями объектов**" на стр. 654)

Удаление объектов из списка удаленных объектов

Только пользователи с правами **Изменение** для области **Удаленные объекты** могут удалять объекты из списка удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей на стр. 648).

► *Чтобы удалить объект из списка удаленных объектов, выполните следующие действия:*

1. В дереве консоли выберите узел нужного Сервера администрирования и выберите папку **Удаленные объекты**.
2. В рабочей области папки выберите объект или объекты, которые вы хотите удалить.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **DELETE**.
   - В контекстном меню объекта или объектов, которые вы выбрали, выберите пункт **Удалить**.
4. В диалоговом окне нажмите на кнопку **Да**.

Объект удален из списка удаленных объектов. Вся информация объекта (включая все ревизии) удалена из базы данных. Вы не можете восстановить эту информацию.

Дистанционная установка операционных систем и программ

Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ "Лаборатории Касперского" или других производителей программного обеспечения.

Захват образов операционных систем

Kaspersky Security Center может выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета (см. раздел "Создание инсталляционных пакетов программ" на стр. 670).

Для создания образов операционной системы на Сервере администрирования должен быть установлен пакет инструментов Windows Automated Installation Kit (WAIK).

Функциональность захвата образа операционной системы имеет следующие особенности:

- Образ операционной системы нельзя снимать с устройства, на котором установлен Сервер администрирования.
- Во время снятия образа операционной системы происходит обнуление параметров эталонного устройства утилитой sysprep.exe. В случае необходимости восстановления параметров эталонного устройства в мастере создания образа операционной системы необходимо установить флажок **Сохранять резервную копию состояния устройства**.
- В процессе снятия образа выполняется перезагрузка эталонного устройства.

Развертывание образов операционных систем на новых устройствах

Администратор может использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). Администратор назначает устройство в сети, которое будет использоваться в качестве PXE-сервера. Это устройство должно отвечать следующим требованиям:

- на устройстве должен быть установлен Агент администрирования;
- на устройстве не должен работать DHCP-сервер, так как PXE-сервер использует те же порты, что и DHCP;
- в сегменте сети, в который входит устройство, не должно быть других PXE-серверов.

Для развертывания операционной системы необходимо, чтобы на устройстве была установлена сетевая карта, устройство было подключено к сети, а в процессе загрузки устройства в среде BIOS был выбран вариант установки Network boot.

Развертывание операционной системы выполняется в следующей последовательности:

1. PXE-сервер устанавливает соединение с новым клиентским устройством при загрузке клиентского

устройства.

2. Клиентское устройство включается в среду Windows Preinstallation Environment (WinPE).

   Для включения устройства в среду WinPE может потребоваться настройка состава драйверов для среды WinPE.

3. Клиентское устройство регистрируется на Сервере администрирования.
4. Администратор назначает клиентскому устройству инсталляционный пакет с образом операционной системы.

   Администратор может добавлять необходимые драйверы в инсталляционный пакет с образом операционной системы. Администратор также может указывать конфигурационный файл с параметрами операционной системы (файл ответов), которые должны применяться во время установки.

5. Выполняется развертывание операционной системы на клиентском устройстве.

Администратор может вручную указать MAC-адреса еще не подключившихся клиентских устройств и назначить им инсталляционный пакет с образом операционной системы. Когда указанные клиентские устройства подключаются к PXE-серверу, автоматически выполняется установка операционной системы на этих устройствах.

Развертывание образов операционных систем на устройствах с уже установленной операционной системой

Развертывание образов операционной системы на клиентских устройствах, на которых уже установлена рабочая операционная система, выполняется с помощью задачи удаленной установки для наборов устройств.

Установка программ "Лаборатории Касперского" и других производителей программного обеспечения

Администратор может создавать инсталляционные пакеты любых программ, включая программы, указанные пользователем, и устанавливать эти программы на клиентские устройства с помощью задачи удаленной установки.

В этом разделе

Создание образов операционных систем

Создание образов операционных систем выполняется при помощи задачи снятия образа операционной системы эталонного устройства.

► *Чтобы создать задачу снятия образа операционной системы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет с образом операционной системы**.
4. Следуйте далее указаниям мастера.

   В результате работы мастера создается задача Сервера администрирования **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. Задачу можно просмотреть в папке **Задачи**.

В результате выполнения задачи **Создание инсталляционного пакета на основе образа ОС эталонного устройства** создается инсталляционный пакет, который можно использовать для развертывания операционной системы на клиентских устройствах с помощью PXE-сервера или задачи удаленной установки. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

Добавление драйверов для среды предустановки Windows (WinPE)

► *Чтобы добавить драйверы для среды предустановки Windows (WinPE), выполните следующие*

действия:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. В рабочей области папки **Развертывание образов устройств** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить состав драйверов для среды предустановки Windows (WinPE)**.

   В результате откроется окно **Драйверы для среды предустановки Windows**.
3. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор драйвера**.
4. В окне **Выбор драйвера** выберите драйвер из списка.

   Если необходимый драйвер отсутствует в списке, нажмите на кнопку **Добавить** и в открывшемся окне **Добавление драйвера** укажите имя драйвера и папку дистрибутива драйвера.

   Вы можете выбрать папку по кнопке **Обзор**.

   В окне **Добавление драйвера** нажмите на кнопку **ОК**.
5. В окне **Выбор драйвера** нажмите на кнопку **ОК**.

   Драйвер будет добавлен в хранилище Сервера администрирования. Добавленный в хранилище драйвер отображается в окне **Выбор драйвера**.
6. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **ОК**.

Драйвер будет добавлен в среду предустановки Windows (WinPE).

Добавление драйверов в инсталляционный пакет с образом операционной системы

► *Чтобы добавить драйверы в инсталляционный пакет с образом операционной системы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.
3. В окне свойств инсталляционного пакета выберите раздел **Дополнительные драйверы**.
4. В разделе **Дополнительные драйверы** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор драйвера**.
5. В окне **Выбор драйвера** выберите драйверы, которые вы хотите добавить в инсталляционный пакет с образом операционной системы.

Новые драйверы можно добавить в хранилище Сервера администрирования при нажатии на кнопку **Добавить** в окне **Выбор драйвера**.

6. Нажмите на кнопку **ОК**.

Добавленные драйверы отображаются в разделе **Дополнительные драйверы** в окне свойств инсталляционного пакета с образом операционной системы.

Настройка параметров утилиты sysprep.exe

Утилита sysrep.exe используется для подготовки устройства к созданию с него образа операционной системы.

► *Чтобы настроить параметры утилиты sysprep.exe, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.
3. В окне свойств инсталляционного пакета выберите раздел **Параметры sysprep.exe**.
4. В разделе **Параметры sysprep.exe** укажите конфигурационный файл, который будет использоваться при развертывании операционной системы на клиентском устройстве:
   - **Использовать конфигурационный файл по умолчанию**. Выберите этот вариант, чтобы использовать файл ответов, создаваемый по умолчанию во время снятия образа операционной системы.
   - **Задать пользовательские значения основных параметров**. Выберите этот вариант, чтобы задать значения параметров с помощью пользовательского интерфейса.
   - **Задать конфигурационный файл**. Выберите этот вариант, чтобы использовать собственный файл ответов.
5. Нажмите на кнопку **Применить**, чтобы внесенные изменения вступили в силу.

Развертывание операционных систем на новых устройствах в сети

► *Чтобы развернуть операционную систему на новых устройствах, на которых еще не установлена операционная система, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Управлять списком PXE-серверов в сети**.

   В открывшемся окне **Свойства: Развертывание образов устройств** перейдите в раздел

PXE-серверы.

3. В разделе **PXE-серверы** нажмите на кнопку **Добавить** и в открывшемся окне **PXE-серверы** выберите устройство, которое будет использоваться как PXE-сервер.

   Добавленное устройство отобразится в разделе PXE-серверы.

4. В разделе **PXE-серверы** выберите PXE-сервер и нажмите на кнопку **Свойства**.
5. В окне свойств выбранного PXE-сервера в разделе **Параметры подключения к PXE-серверу** выполните настройку параметров подключения Сервера администрирования к PXE-серверу.
6. Выполните загрузку клиентского устройства, на котором вы хотите развернуть операционную систему.
7. В среде BIOS клиентского устройства выберите вариант установки Network boot.

   Клиентское устройство подключается к PXE-серверу и отображается в рабочей области папки **Развертывание образов устройств**.

8. В блоке **Действия** по ссылке **Назначить инсталляционный пакет** выберите инсталляционный пакет, который будет использоваться для установки операционной системы на выбранное устройство.

   После добавления устройства и назначения для него инсталляционного пакета развертывание операционной системы на этом устройстве начинается автоматически.

9. Для отмены развертывания операционной системы на клиентском устройстве воспользуйтесь ссылкой **Отменить установку образов ОС** в блоке **Действия**.

► *Чтобы добавить устройства по MAC-адресу, выполните одно из следующих действий:*

- по ссылке **Добавить MAC-адрес устройства** в папке **Развертывание образов устройств** откройте окно **Новое устройство** и укажите MAC-адрес устройства, которое вы хотите добавить;
- по ссылке **Импортировать MAC-адреса устройств из файла** в папке **Развертывание образов устройств** выберите файл, содержащий список MAC-адресов всех устройств, на которых вы хотите развернуть операционную систему.

Развертывание операционных систем на клиентских устройствах

► *Чтобы выполнить развертывание операционной системы на клиентских устройствах с уже установленной операционной системой, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет с образом операционной системы.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки операционной системы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Создание инсталляционных пакетов программ

► *Чтобы создать инсталляционный пакет программы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на одну из кнопок:
   - **Создать инсталляционный пакет для программы "Лаборатории Касперского"**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы "Лаборатории Касперского".
   - **Создать инсталляционный пакет для программы, указанной пользователем**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы с помощью исполняемого файла. Как правило, исполняемый файл является установочным файлом программы.
     - **Копировать всю папку в инсталляционный пакет.**

       Выберите этот параметр, если исполняемый файл сопровождается дополнительными файлами, необходимыми для установки программы. Прежде чем включить этот параметр, убедитесь, что все требуемые файлы хранятся в одной папке. Если этот параметр включен, программа добавляет все содержимое папки, включая указанный исполняемый файл, в установочный пакет.
     - **Указать параметры установки**

       Чтобы удаленная установка прошла успешно, большинство программ требуют, чтобы установка проводилась в автоматическом режиме. В этом случае вы должны указать параметры автоматической установки.

       Настройте параметры установки:
       - **Параметры запуска исполняемого файла.**

         Если программе требуются дополнительные параметры для установки без вывода сообщений, укажите их в этом поле. Дополнительную информацию см. в документации производителя.

         Вы также можете указать и другие параметры.
       - **Конвертировать параметры на рекомендуемые значения для программ, распознаваемых Kaspersky Security Center 11.**

         Программа будет установлена с рекомендуемыми параметрами, если информация об указанной программе содержится в базе данных "Лаборатории Касперского".

         Если вы ввели параметры в поле Параметры запуска исполняемого файла, они будут изменены на рекомендуемые параметры.

         По умолчанию параметр включен.

         База данных "Лаборатории Касперского" создана и поддерживается аналитиками

"Лаборатории Касперского". Для каждой программы, добавляемой в базу данных, аналитики "Лаборатории Касперского" определяют оптимальные параметры установки. Параметры определяются так, чтобы обеспечить успешную удаленную установку программы на клиентское устройство. База данных обновляется автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования.

- **Выбрать программу из базы "Лаборатории Касперского" для создания инсталляционного пакета**. Выберите этот вариант, если вы хотите выбрать программу стороннего производителя из базы "Лаборатории Касперского", для которой требуется создать инсталляционный пакет. База данных создается автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования (см. раздел "Создание задачи для загрузки обновлений в хранилище Сервера администрирования" на стр. 362); программы отображаются в списке.
- **Создать инсталляционный пакет с образом операционной системы**. Выберите этот вариант, если вы хотите создать инсталляционный пакет с образом операционной системы эталонного устройства.

  В результате работы мастера создается задача Сервера администрирования с названием **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. В результате выполнения этой задачи создается инсталляционный пакет, который можно использовать для развертывания образа операционной системы с помощью PXE-сервера или задачи удаленной установки.

4. Следуйте далее указаниям мастера.

В результате работы мастера создается инсталляционный пакет, который можно использовать для установки программы на клиентские устройства. Вы можете просмотреть инсталляционные пакеты, выбрав папку **Инсталляционные пакеты** в дереве консоли.

См. также:

Создание инсталляционного пакета..... 285

Выписка сертификата для инсталляционных пакетов программ

► *Чтобы выписать сертификат для инсталляционного пакета программы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.

   В результате откроется окно свойств папки **Инсталляционные пакеты**.

3. В окне свойств папки **Инсталляционные пакеты** выберите раздел **Подпись автономных пакетов**.
4. В разделе **Подпись автономных пакетов** нажмите на кнопку **Задать**.

   В результате откроется окно **Сертификат**.
5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:
   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509-сертификат**:
     a. укажите файл закрытого ключа (файл с расширением prk или pem);
     b. укажите пароль закрытого ключа;
     c. укажите файл открытого ключа (файл с расширением cer).
6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для инсталляционного пакета программы.

Установка программ на клиентские устройства

► *Чтобы установить программу на клиентские устройства, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет программы, которую вы хотите установить.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки программы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Вы можете устанавливать Агент администрирования на клиентские устройства с операционными системами Windows, Linux и MacOS с помощью мастера развертывания защиты.
Чтобы управлять 64-разрядными программами безопасности с помощью Kaspersky Security Center на устройствах с операционными системами Linux, необходимо использовать 64-разрядный Агент администрирования для Linux. Требуемую версию Агента администрирования можно загрузить с веб-сайта Службы технической поддержки https://support.kaspersky.ru.
Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux необходимо подготовить устройство (см. раздел "Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования" на стр. 293).

Управление мобильными устройствами

Управление защитой мобильными устройствами через Kaspersky Security Center выполняется с помощью компонента Управление мобильными устройствами. Если вы планируете управлять мобильными устройствами, принадлежащими сотрудникам вашей организации, вы должны включить Управление мобильными устройствами.

В этом разделе приведены инструкции по включению, настройке и отключению Управления мобильными устройствами. В этом разделе также описано управление мобильными устройствами, подключенными к Серверу администрирования.

В этом разделе

Сценарий: Развертывание Управления мобильными устройствами

В этом разделе приведен сценарий для настройки возможностей Управления мобильными устройствами в Kaspersky Security Center.

Требования

Убедитесь, что ваша лицензия предоставляет доступ к возможностям Управления мобильными устройствами.

Развертывание поддержки Управления мобильными устройствами содержит следующие шаги:

a. **Подготовка портов**

Убедитесь, что на Сервере администрирования доступен порт 13292. Этот порт требуется для подключения мобильных устройств (см. раздел "Порты, используемые Kaspersky Security Center" на стр. 56). Также вы можете сделать доступным порт 17100. Этот порт требуется только для активации

прокси-сервера для управляемых мобильных устройств; если управляемые мобильные устройства имеют доступ в интернет, этот порт доступным делать не требуется.

b. **Включение Управления мобильными устройствами**

   При наличии специальной лицензии Управление мобильными устройствами можно включить во время запуска мастера первоначальной настройки Сервера администрирования или позже (см. раздел "Включение Управления мобильными устройствами" на стр. 676).

c. **Указание внешнего адреса Сервера администрирования**

   Вы можете указать внешний адрес во время запуска мастера первоначальной настройки Сервера администрирования или позже. Если вы не выбрали Управление мобильными устройствами для установки и не указали адрес в мастере установки программы, укажите внешний адрес в свойствах инсталляционного пакета.

d. **Добавление мобильных устройств в группу Управляемые устройства**

   Добавьте мобильные устройства в группу Управляемые устройства, чтобы управлять этими устройствами с помощью политик. Вы можете создать правило перемещения на одном из шагов мастера первоначальной настройки Сервера администрирования. Также вы можете создать правило перемещения позже. Если вы не создадите такое правило, вы можете добавить мобильные устройства в группу Управляемые устройства вручную.

   Вы можете добавить мобильные устройства в группу Управляемые устройства напрямую или создать для них подгруппу (или несколько подгрупп).

   Позже, в любое время вы можете подключить новое мобильное устройство к Серверу администрирования с помощью мастера подключения нового мобильного устройства (см. раздел "Добавление мобильных устройств в список управляемых устройств" на стр. 693).

e. **Создание политики для мобильных устройств**

   Чтобы управлять мобильными устройствами, создайте политику (или несколько политик) для них в соответствующих подгруппах. Вы можете изменить параметры политики в любое время.

Результаты

После завершения сценария, вы сможете управлять Android и iOS устройствами, используя Kaspersky Security Center.

О групповой политике управления EAS и iOS MDM-устройствами

Для управления iOS MDM и EAS-устройствами вы можете использовать плагин управления управления Kaspersky Device Management для iOS, входящий в комплект поставки Kaspersky Security Center. Kaspersky Device Management для iOS позволяет создавать групповые политики для настройки конфигурационных параметров iOS MDM и EAS-устройств без использования iPhone® Configuration Utility и профиля управления Exchange Active Sync.

Групповая политика управления EAS и iOS MDM-устройствами предоставляет администратору следующие возможности:

- для управления EAS-устройствами:
  - настраивать параметры пароля для разблокирования устройства;
  - настраивать хранение данных на устройстве в зашифрованном виде;
  - настраивать параметры синхронизации корпоративной почты;
  - настраивать аппаратные функции мобильных устройств, например, использование съемных дисков, использование камеры, использование Bluetooth;
  - настраивать ограничения для использования мобильных приложений на устройстве.
- для управления iOS MDM-устройствами:
  - настраивать параметры безопасности использования пароля на устройстве;
  - настраивать ограничения для использования аппаратных функций устройства, а также ограничения на установку, удаление мобильных приложений;
  - настраивать ограничения для использования на устройстве встроенных мобильных приложений, например, YouTube™, iTunes® Store, Safari;
  - настраивать ограничения просмотра медиаконтента (например, фильмов и тв-шоу) по региону местоположения устройства;
  - настраивать параметры подключения устройства к интернету через прокси-сервер (Глобальный HTTP-прокси);
  - настраивать параметры единой учетной записи, с помощью которой пользователь может получить доступ к корпоративным приложениям и сервисам (технология единого входа);
  - контролировать использование интернета (посещение веб-сайтов) на мобильных устройствах;
  - настраивать параметры беспроводных сетей (Wi-Fi), точек доступа (APN), виртуальных частных сетей (VPN) с использованием различных механизмов аутентификации и сетевых протоколов;
  - настраивать параметры подключения к устройствам AirPlay® для потоковой передачи фотографий, музыки и видео;
  - настраивать параметры подключения к принтерам AirPrint™ для печати документов с устройства беспроводным способом;
  - настраивать параметры синхронизации с сервером Microsoft Exchange, а также учетные записи пользователей для использования корпоративной почты на устройствах;
  - настраивать учетные данные пользователя для синхронизации со службой каталогов LDAP;
  - настраивать учетные данные пользователя для подключения к сервисам CalDAV и CardDAV, что позволяет пользователю использовать корпоративные календари и списки контактов;
  - настраивать параметры интерфейса iOS на устройстве пользователя, например, шрифты или иконки для избранных веб-сайтов;

- добавлять новые сертификаты безопасности на устройство;
- настраивать параметры SCEP-сервера для автоматического получения устройством сертификатов из Центра сертификации;
- добавление собственных параметров для работы мобильных приложений.

Особенностью политики управления EAS и iOS MDM-устройствами является то, что она назначается на группу администрирования, в которую входят Сервер мобильных устройств iOS MDM и Сервер мобильных устройств Exchange ActiveSync (далее серверы мобильных устройств). Все параметры, заданные в этой политике, вначале распространяются на серверы мобильных устройств, затем на мобильные устройства, которыми они управляют. В случае использования иерархической структуры групп администрирования подчиненные серверы мобильных устройств получают параметры политики с главных серверов мобильных устройств и распространяют их на мобильные устройства.

Подробные сведения о работе групповой политики управления EAS и iOS MDM-устройствами в Консоли администрирования Kaspersky Security Center приведены в онлайн-справке Kaspersky Security 10 для мобильных устройств https://help.kaspersky.com/KESMob/10SP3MR1/ru-RU/141410.htm.

Включение Управления мобильными устройствами

Для управления мобильными устройствами необходимо включить Управление мобильными устройствами. Если вы не включили Управление мобильными устройствами в мастере первоначальной настройки, вы можете сделать это позже (см. раздел "Мастер первоначальной настройки Сервера администрирования" на стр. 213). Управление мобильными устройствами требует лицензии (см. раздел "Варианты лицензирования Kaspersky Security Center" на стр. 257).

Включение Управления мобильными устройствами доступно только на главном Сервере администрирования.

► *Чтобы включить Управление мобильными устройствами, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки нажмите на кнопку **Включить Управление мобильными устройствами**. Эта кнопка доступна, только если вы ранее не включали **Управление мобильными устройствами**.

   Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.
3. Выберите пункт **Включить Управление мобильными устройствами**, чтобы управлять мобильными устройствами.
4. В окне **Выбор способа активации программы** произведите активацию программы с помощью файла ключа или кода активации (см. раздел "Шаг 2.Выбор способа активации программы" на стр. 215).

   Управление мобильными устройствами будет недоступно, пока вы не активируете возможность

Управления мобильными устройствами.

5. В окне **Параметры прокси-сервера для доступа к сети Интернет** установите флажок **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если флажок установлен, становятся доступны поля ввода параметров. Настройте параметры подключения к прокси-сервер (см. раздел "Шаг 3. Настройка параметров прокси-сервера" на стр. 216).
6. В окне **Проверка обновлений для плагинов и инсталляционных пакетов** выберите один из следующих вариантов:
   - **Проверить актуальность плагинов и инсталляционных пакетов**

     Запуск проверки на актуальность. Если проверка обнаружит использование устаревших версий плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.
   - **Пропустить проверку**

     Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Этот вариант можно выбрать, например, если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить пользоваться устаревшей версией программы.

   Пропуск проверки актуальности плагинов может привести к некорректной работе программы.
7. В окне **Доступные последние версии плагинов** загрузите и установите последние версии плагинов на необходимом вам языке. Для обновления плагина не требуется лицензии.

   После установки плагинов и пакетов программа проверяет, все ли необходимые плагины для корректной работы мобильных устройств были установлены. Если обнаружено использование устаревших версий плагинов, мастер предложит загрузить актуальные версии вместо устаревших.
8. В окне **Параметры подключения мобильных устройств** настройте порты Сервера администрирования (см. раздел "Шаг 9. Подключение мобильных устройств" на стр. 220).

После завершения работы мастера будут выполнены следующие изменения:

- создана политика Kaspersky Endpoint Security для Android;
- создана политика Kaspersky Device Management для iOS;
- открыты порты Сервера администрирования для мобильных устройств.

Изменение параметров Управления мобильными устройствами

► *Чтобы включить поддержку мобильных устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

2. В рабочей области папки перейдите по ссылке **Порты подключения для мобильных устройств**.

   Отобразится раздел **Дополнительные порты** окна свойств Сервера администрирования.

3. В разделе **Дополнительные порты** измените необходимые вам параметры:

   - **SSL-порт для прокси-сервера активации**

     Номер SSL-порта для подключения Kaspersky Endpoint Security для Windows к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17000.

   - Открыть порт для мобильных устройств

     Открывается порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

     По умолчанию параметр включен.

   - Порт для синхронизации мобильных устройств

     Номер порта, по которому мобильные устройства подключаются к Серверу администрирования и обмениваются с ним информацией. По умолчанию установлен порт 13292.

     Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.

   - **Порт для активации мобильных устройств**

     Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17100.

4. Нажмите на кнопку **ОК**.

Выключение Управления мобильными устройствами

Выключение Управления мобильными устройствами доступно только на главном Сервере администрирования.

► *Чтобы выключить поддержку мобильных устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки перейдите по ссылке **Настроить дополнительные компоненты**.

   Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Выберите пункт **Не включать Управление мобильными устройствами**, если вы больше не хотите

управлять мобильными устройствами.

4. Нажмите на кнопку **ОК**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования. Порт подключения мобильных устройств и порт активации мобильных устройств будут закрыты автоматически.

Созданные политики Kaspersky Endpoint Security для Android и Kaspersky Device Management для iOS не будут удалены. Правила выпуска сертификатов не изменяются. Установленные плагины не удаляются. Правило перемещения мобильных устройств не будет удалено.

После повторного включения Управления мобильными устройствами на управляемых мобильных устройствах может потребоваться переустановка мобильных приложений, которые необходимы для управления мобильными устройствами.

Работа с командами для мобильных устройств

Этот раздел содержит информацию о командах для управления мобильными устройствами, которые поддерживает программа. В разделе приведены инструкции по отправке команд на мобильные устройства, а также по просмотру статуса выполнения команд в журнале команд.

В этом разделе

Команды для управления мобильными устройствами

Kaspersky Security Center поддерживает команды для управления мобильными устройствами.

Команды используются для дистанционного управления мобильными устройствами. Например, в случае потери мобильного устройства с помощью команды можно удалить корпоративные данные с устройства.

Вы можете использовать команды для следующих типов управляемых мобильных устройств:

- iOS MDM-устройства;
- KES-устройства;
- EAS-устройства.

Каждый тип устройства поддерживает свой набор команд.

Особенности некоторых команд

- Для всех типов устройств в случае успешного выполнения команды **Сбросить настройки до заводских** все данные будут удалены с устройства, настройки устройства будут сброшены до заводских.
- Для iOS MDM-устройств в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
- Для KES-устройств в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google™. Для KES-устройств дополнительно будут удалены данные с карты памяти.
- Перед отправкой команды **Определить местоположение** на KES-устройство вам потребуется подтвердить, что вы используете эту команду для санкционированного поиска потерянного устройства, принадлежащего вашей организации или одному из сотрудников. При использовании Kaspersky Security Center версии Service Pack 2 Maintenance Release 1 и более ранних версий мобильное устройство, на которое отправлена команда **Определить местоположение**, блокируется. Начиная с версии Kaspersky Security Center 10 Service Pack 3 блокировка устройства не происходит.

Список команд для мобильных устройств

В таблице ниже приведен список команд для каждого типа устройства.

Таблица 61. Список поддерживаемых команд

Тип мобильного устройства	Команды	Результат выполнения команды
iOS MDM-устройство	Заблокировать	Мобильное устройство заблокировано.
	Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.
	Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.

Тип мобильного устройства	Команды	Результат выполнения команды
	Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.
	Установить профиль	Конфигурационный профиль установлен на мобильное устройство.
	Удалить профиль	Конфигурационный профиль удален с мобильного устройства.
	Установить provisioning-профиль	Provisioning-профиль установлен на мобильное устройство.
	Удалить provisioning-профиль	Provisioning-профиль удален с мобильного устройства.
	Установить приложение	Приложение установлено на мобильное устройство.
	Удалить приложение	Приложение удалено с мобильного устройства.
	Вести код погашения	Введен код погашения для платного приложения.
	Настроить роуминг	Включен или выключен роуминг данных и голосовой роуминг.
KES-устройство	Заблокировать	Мобильное устройство заблокировано.
	Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.
	Удалить корпоративные данные	Удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google. Удалены данные с карты памяти.
	Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.

Тип мобильного устройства	Команды	Результат выполнения команды
	Определить местоположение	Местоположение мобильного устройства определено и показано на Google Картах™. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства и сохранена на Сервере администрирования. Фотографии доступны для просмотра в журнале команд. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал.
EAS-устройство	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.

Использование Google Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций. Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Google Firebase Cloud Messaging. В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Google Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Google Firebase Cloud Messaging администратору необходимо иметь учетную запись Google. Более подробную информацию о получении параметров Google Firebase Cloud Messaging см. в статье Базы знаний на веб-сайте Службы технической поддержки http://support.kaspersky.ru/11770.

► *Чтобы настроить параметры Google Firebase Cloud Messaging, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.

   В результате откроется окно свойств папки **Мобильные устройства**.
3. Выберите раздел **Параметры Google Firebase Cloud Messaging**.

4. В поле **Идентификатор отправителя** укажите номер проекта Google API, полученный вами при создании проекта в консоли разработчика Google.
5. В поле **Ключ сервера** введите обычный ключ сервера, который вы создали в консоли разработчика Google.

При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Google Firebase Cloud Messaging.

Вы можете изменить параметры Google Firebase Cloud Messaging по кнопке **Сбросить параметры**.

Отправка команд

► *Чтобы отправить команду на мобильное устройство пользователя, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. Выберите мобильное устройство пользователя, на которое нужно отправить команду.
3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
4. В окне **Команды для управления мобильным устройством** перейдите в раздел с названием команды, которую нужно отправить на мобильное устройство, и нажмите на кнопку **Отправить команду**.

   В зависимости от выбранной команды после нажатия на кнопку **Отправить команду** может открыться окно настройки дополнительных параметров команды. Например, при отправке команды на удаление с мобильного устройства provisioning-профиля программа предлагает выбрать provisioning-профиль, который нужно удалить с мобильного устройства. Укажите в окне дополнительные параметры команды и подтвердите свой выбор. После этого команда будет отправлена на мобильное устройство.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Просмотр статусов команд в журнале команд

Программа сохраняет информацию о всех командах, отправленных на мобильные устройства, в журнале команд. В журнале команд сохраняется информация о времени и дате отправления команд на мобильное устройство, статусы команд, а также подробные описания результатов выполнения команд. Например, в

случае неудачного выполнения команды в журнале отображается причина ошибки. Записи в журнале команд хранятся не более 30 дней.

Команды, отправленные на мобильные устройства, могут иметь следующие статусы:

- *Выполняется* – команда отправлена на мобильное устройство.
- *Завершена* – выполнение команды успешно завершено.
- *Завершена с ошибкой* – выполнить команду не удалось.
- *Удаляется* – команда удаляется из очереди команд, отправленных на мобильное устройство.
- *Удалена* – команда успешно удалена из очереди команд, отправленных на мобильное устройство.
- *Удаление завершено с ошибкой* – команду не удалось удалить из очереди команд, отправленных на мобильное устройство.

Программа ведет журнал команд для каждого мобильного устройства.

► *Чтобы просмотреть журнал команд, отправленных на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. Выберите в списке мобильное устройство, для которого вы хотите просмотреть журнал команд.
3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

   Откроется окно **Команды для управления мобильным устройством**. Разделы окна **Команды для управления мобильным устройством** соответствуют командам, которые можно отправить на мобильное устройство.
4. Выбирайте разделы с нужными вам командами и просматривайте информацию об отправке и выполнении команд в блоке **Журнал команд**.

В блоке **Журнал команд** можно просмотреть список команд, отправленных на мобильное устройство, и информацию о командах. С помощью фильтра **Показать команды** можно показывать в списке только команды с выбранным статусом.

Работа с сертификатами

Этот раздел содержит информацию о работе с сертификатами мобильных устройств. В разделе приведены инструкции по установке сертификатов на мобильные устройства пользователей и по настройке правил выписки сертификатов. Раздел также содержит инструкции по интеграции программы с инфраструктурой открытых ключей и по настройке поддержки Kerberos.

В этом разделе

Установка сертификата

Вы можете устанавливать на мобильное устройство пользователя сертификаты следующих типов:

- общие сертификаты для идентификации мобильного устройства;
- почтовые сертификаты для настройки на мобильном устройстве корпоративной почты;
- VPN-сертификат для настройки на мобильном устройстве доступа к виртуальной частной сети.

► *Чтобы установить сертификат на мобильное устройство пользователя, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по ссылке **Добавить сертификат** запустите мастер установки сертификата.

Следуйте далее указаниям мастера.

В результате работы мастера сертификат будет создан, добавлен в список сертификатов пользователя, кроме того, будет отправлено уведомление пользователю со ссылкой для загрузки и установки сертификата на мобильное устройство. Список всех сертификатов можно просмотреть и экспортировать в файле (см. раздел "Просмотр списка сертификатов выписанных пользователю" на стр. 654). Можно удалять и перевыпускать сертификаты, а также просматривать их свойства.

Шаг 1. Тип сертификата

Укажите тип сертификата, который необходимо установить на мобильное устройство пользователя:

- **Мобильный сертификат** – для идентификации мобильного устройства.
- **Почтовый сертификат** – для настройки на мобильном устройстве корпоративной почты.
- **VPN-сертификат** – для настройки на мобильном устройстве доступа к виртуальной частной сети.

Шаг 2. Тип устройства

Это окно отображается, только если ранее был выбран (см. раздел "Шаг 1. Тип сертификата" на стр. 686) тип сертификата **Почтовый сертификат** или **VPN-сертификат**.

Укажите тип операционной системы устройства:

- **iOS MDM-устройство**. Выберите этот вариант, если необходимо установить сертификат на мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM.
- **KES-устройство под управлением Kaspersky Security для мобильных устройств**. Выберите этот вариант, если необходимо установить сертификат на KES-устройство. В этом случае сертификат будет использоваться при подключении к Серверу администрирования для идентификации пользователя.
- **KES-устройство, которое подключается к Серверу администрирования без аутентификации по сертификату пользователя**. Выберите этот вариант, если необходимо установить сертификат на KES-устройство без аутентификации по сертификату. В этом случае на последнем шаге мастера в окне **Способ уведомления пользователей** администратор должен выбрать тип авторизации пользователя при подключении к Серверу администрирования.

Шаг 3. Выбор пользователя

Выберите в списке пользователей, группы пользователей или группы пользователей Active Directory, для которых вы хотите установить сертификат.

В окне **Пользовательская выборка** можно выполнить поиск внутренних пользователей Kaspersky Security Center. Вы можете нажать на кнопку **Добавить**, чтобы добавить внутреннего пользователя.

Шаг 4. Источник сертификата

В окне можно выбрать источник сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Можно задать сертификат одним из следующих способов:

- Автоматически создать сертификат средствами Сервера администрирования и доставить сертификат на устройство.
- Укажите файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге

было выбрано несколько пользователей.

Установите флажок **Опубликовать сертификат**, если необходимо отправить уведомление пользователю о создании сертификата для его мобильного устройства.

Если мобильное устройство пользователя уже было авторизовано по сертификату ранее и нет необходимости указывать имя учетной записи и пароль для получения нового сертификата, снимите флажок **Опубликовать сертификат**. В этом случае окно **Способ уведомления пользователя** отображаться не будет.

Шаг 5. Тег сертификата

Окно **Тег сертификата** отображается, если в окне **Тип устройства** был выбран вариант **iOS MDM-устройство**.

В раскрывающемся списке вы можете назначить тег для сертификата iOS MDM-устройства пользователя. Сертификат с назначенным тегом может иметь специальные параметры, установленные для этого тега в свойствах политики Kaspersky Device Management для iOS.

Для выбора в раскрывающемся списке доступны теги *Шаблон сертификата 1*, *Шаблон сертификата 2* и *Шаблон сертификата 3*, параметры которых могут быть настроены в следующих разделах: Вы можете настроить теги в следующих разделах:

- Если в окне **Тип сертификата** был выбран тип **Почтовый сертификат**, параметры тегов для него настраиваются в свойствах учетной записи Exchange ActiveSync для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS → Раздел **Exchange ActiveSync** → **Добавить** → **Дополнительно**).
- Если в окне **Тип сертификата** был выбран тип **VPN-сертификат**, параметры тегов для него настраиваются в свойствах сети VPN для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS →Раздел **VPN** → **Добавить** → **Дополнительно**). Настройка тегов, используемых для VPN-сертификатов, недоступна, если для сети VPN выбран тип соединения L2TP, PPTP, или IPSec (Cisco™).

См. также:

Установка сертификата пользователю.....653

Шаг 6. Параметры публикации сертификата

В этом окне вы можете указать следующие параметры публикации сертификата:

- **Не уведомлять пользователя о новом сертификате**

Включите этот параметр, если вы не хотите отправлять пользователю уведомление о создании сертификата для его мобильного устройства. В этом случае окно **Способ уведомления пользователя** отображаться не будет.

Этот параметр применим только к устройствам с установленным приложением Kaspersky Endpoint Security для Android.

Возможно, вы захотите включить этот параметр, например, если мобильное устройство пользователя уже было идентифицировано с помощью сертификата, поэтому нет необходимости указывать имя учетной записи и пароль для получения нового сертификата.

- **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленным Kaspersky Endpoint Security для Android)**

Включите этот параметр, чтобы Kaspersky Security Center автоматически повторно отправлял сертификат каждый раз, когда срок его действия истекает в ближайшее время или не найден на целевом устройстве.

Сертификат автоматически отправляется повторно за несколько дней до истечения срока действия сертификата. Вы можете установить количество дней в окне Правила выпуска сертификатов (см. раздел "Настройка правил выпуска сертификатов" на стр. 690).

В некоторых случаях сертификаты не могут быть найдены на устройствах. Например, это может произойти, если пользователь заново установит приложение безопасности "Лаборатории Касперского" на устройство или сбросит настройки устройства до заводских. В этом случае Kaspersky Security Center проверяет идентификатор устройства при следующей попытке устройства подключиться к Серверу администрирования. Если устройство имеет такой же идентификатор, как и при выдаче сертификата, программа передает сертификат на устройство.

Шаг 7. Способ уведомления пользователей

Окно не отображается, если вы выбрали (см. раздел "Шаг 2. Тип устройства" на стр. 686) тип устройства **iOS MDM-устройство** или, если вы выбрали (см. раздел "Шаг 6. Параметры публикации сертификата" на стр. 687) параметр **Не уведомлять пользователя о новом сертификате**.

В окне **Способ уведомления пользователя** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство.

В поле **Пароль пользователя** укажите тип аутентификации пользователя:

- **Учетные данные (доменные или псевдонима)**

  В этом случае пользователь использует доменный пароль или пароль внутреннего пользователя Kaspersky Security Center, для того чтобы получить новый сертификат.

- **Одноразовый пароль**

В этом случае пользователь получит одноразовый пароль, который будет выслан на электронную почту или

с помощью SMS. Этот пароль необходимо будет указать для получения нового сертификата.

Этот параметр изменится на **Пароль**, если вы включили параметр **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленными приложениями безопасности "Лаборатории Касперского")** в окне **Параметры публикации сертификатов**.

- **Пароль.**

В этом случае пароль используется каждый раз, когда сертификат отправляется пользователю.

Этот параметр изменится на **Одноразовый пароль**, если вы включили параметр **Разрешить устройству получать один и тот же сертификат несколько раз (только для устройств с установленными приложениями безопасности "Лаборатории Касперского")** в окне **Параметры публикации сертификатов**.

Это поле отображается, если вы выбрали **Мобильный сертификат** в окне **Тип сертификата** или если вы выбрали параметр **KES-устройство, которое подключается к Серверу администрирования без аутентификации по сертификату пользователя** как тип устройства.

Выберите вариант уведомления пользователя:

- **Показать пароль после завершения работы мастера**

Если вы выберете этот параметр, имя пользователя, SAM-имя пользователя (Security Account Manager) и пароль для получения сертификата для каждого из выбранных пользователей будут отображаться на последнем шаге мастера установки сертификата. Настройка параметров уведомления пользователя об установленном сертификате будет недоступна.

Если вы добавляете сертификаты для нескольких пользователей, вы можете сохранить предоставленные учетные данные в файл, нажав на кнопку **Экспорт** на последнем шаге мастера установки сертификата.

Этот параметр недоступен, если вы выбрали **Учетные данные (доменные или псевдонима)** на шаге **Способ уведомления пользователя** мастера установки сертификата.

- **Сообщить пользователю о новом сертификате**

  При выборе этого варианта вы можете настроить параметры уведомления пользователя о новом сертификате.

  - **С помощью электронной почты**

    В блоке параметров По электронной почте вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер (см. раздел "Шаг 6. Настройка параметров отправки почтовых уведомлений" на стр. 218).

    Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

- **С помощью SMS**

  В этом блоке параметров вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

  Перейдите по ссылке **Изменить сообщение**, чтобы просмотреть и изменить сообщение, если это необходимо.

См. также:

Установка сертификата пользователю.....653

Шаг 8. Генерация сертификата

На этом шаге создается сертификат. Вы можете нажать на кнопку **Экспорт**, чтобы экспортировать сертификат в папку.

Вы можете нажать на кнопку **Готово**, чтобы выйти из мастера.

Сгенерированный сертификат отображается в списке сертификатов в рабочей области папки **Сертификаты**.

Настройка правил выпуска сертификатов

Сертификаты используются для аутентификации устройств на Сервере администрирования. Все управляемые мобильные устройства должны иметь сертификаты. Можно настроить способ выпуска сертификатов.

► *Чтобы настроить правила выпуска сертификатов, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
3. Перейдите в раздел с названием типа сертификата:

   Выпуск мобильных сертификатов – для настройки выпуска сертификатов для мобильных устройств.

   Выпуск почтовых сертификатов – для настройки выпуска почтовых сертификатов.

   Выпуск VPN-сертификатов – для настройки выпуска VPN-сертификатов.
4. В блоке **Параметры выпуска** настройте выпуск сертификата:
   - Укажите срок действия сертификата в днях.
   - Выберите источник сертификатов (**Сервер администрирования** или **Сертификаты задаются**

вручную).

По умолчанию источником сертификатов выбран Сервер администрирования.

- Задайте шаблон сертификатов (**Шаблон по умолчанию**, **Другой шаблон**).

  Настройка шаблонов доступна, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей (см. стр. 691).

5. В блоке **Параметры автоматического обновления** настройте автоматическое обновление сертификата:

   - В поле **Обновлять, когда до истечения срока действия осталось (сут)** укажите, за какое количество дней до истечения срока действия нужно обновлять сертификат.
   - Чтобы включить автоматическое обновление сертификатов, установите флажок **Автоматически перевыпускать сертификат, если это возможно**.

   Мобильный сертификат можно перевыпускать только вручную.

6. В блоке **Защита паролем** включите и настройте использование пароля при расшифровке сертификатов.

   Защита паролем доступна только для мобильных сертификатов.

   a. Установите флажок **Запрашивать пароль при установке сертификата**.

   b. С помощью ползунка настройте максимальное количество символов в пароле для шифрования.

7. Нажмите на кнопку **ОК**.

Интеграция с инфраструктурой открытых ключей

Интеграция программы с инфраструктурой открытых ключей (Public Key Infrastructure, PKI) необходима для упрощения выписки доменных сертификатов пользователей. В результате интеграции выписка сертификатов происходит автоматически.

Минимально поддерживаемая версия сервера PKI – Windows Server 2008.

Для интеграции с PKI необходимо настроить учетную запись. Учетная запись должна соответствовать следующим требованиям:

- быть доменным пользователем и администратором устройства, на котором установлен Сервер администрирования;
- иметь привилегию SeServiceLogonRight на устройстве с установленным Сервером администрирования.

Под настроенной учетной записью нужно хотя бы один раз выполнить вход на устройстве с установленным Сервером администрирования для того, чтобы создать постоянный профиль пользователя. В хранилище

сертификатов этого пользователя, на устройстве с Сервером администрирования, необходимо установить сертификат агента регистрации, предоставленный администраторами домена.

► *Чтобы настроить интеграцию с инфраструктурой открытых ключей, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области по кнопке **Интегрировать с инфраструктурой открытых ключей** откройте раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

   В результате откроется раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.
3. Установите флажок **Интегрировать выписку сертификатов с PKI**.
4. В поле **Учетная запись** укажите имя учетной записи пользователя, которая будет использоваться для интеграции с инфраструктурой открытых ключей.
5. В поле **Пароль** укажите доменный пароль учетной записи.
6. В списке **Имя шаблона сертификата в системе PKI** выберите шаблон сертификата, который будет использоваться для выпуска сертификатов пользователям домена.

   Под указанной учетной записью в Kaspersky Security Center запускается специализированная служба. Эта служба отвечает за выпуск доменных сертификатов пользователей. Служба запускается, когда происходит загрузка списка шаблонов сертификатов по кнопке **Обновить список**, или при выпуске сертификата.
7. Нажмите на кнопку **ОК**, чтобы сохранить параметры.

В результате интеграции выписка сертификатов происходит автоматически.

Включение поддержки Kerberos Constrained Delegation

Программа поддерживает использование Kerberos Constrained Delegation.

► *Чтобы включить поддержку Kerberos Constrained Delegation, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.
5. В окне свойств Сервера iOS MDM выберите раздел **Параметры**.
6. В разделе **Параметры** установите флажок **Обеспечить совместимость с Kerberos constrained delegation**.
7. Нажмите на кнопку **ОК**.

Добавление мобильных устройств в список управляемых устройств

Чтобы добавить мобильное устройство пользователя в список управляемых устройств, на устройство нужно доставить и установить общий сертификат (см. раздел "Работа с сертификатами" на стр. 684). Общие сертификаты используются для идентификации мобильных устройств Сервером администрирования. После доставки и установки общего сертификата на мобильном устройстве оно отображается в списке управляемых устройств. Добавление мобильных устройств пользователей в список управляемых устройств выполняется с помощью мастера.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser. Соответствующие функции Kaspersky Security Center могут работать некорректно.

Запуск мастера добавления нового устройства

► *Чтобы запустить мастер добавления нового мобильного устройства пользователю, выполните одно из следующих действий:*

- Запустите мастер с помощью контекстного меню в папке **Учетные записи пользователей**:
  1. В дереве консоли выберите папку **Учетные записи пользователей**.

     По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
  2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.
  3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

     Запустится мастер добавления мобильных устройств.
- Запустите мастер по кнопке **Добавить мобильное устройство** в папке **Мобильные устройства**:
  1. В дереве консоли выберите папку **Мобильные устройства**, вложенную в папку **Управление мобильными устройствами**.
  2. В рабочей области папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.
  3. Запустится мастер добавления мобильных устройств.
  4. В окне **Операционная система** выберите тип операционной системы мобильного устройства (Android, iOS).

     Ваши дальнейшие действия в мастере добавления мобильных устройств зависят от того, какой тип операционной системы мобильного устройства вы выбрали (см. инструкции ниже).

Если был выбран способ добавления мобильного устройства с помощью кнопки **Добавить мобильное**

устройство в папке **Мобильные устройства**, в мастере отображается окно **Выбор пользователей**. В окне **Выбор пользователей** выберите пользователей, группы пользователей или группы Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

Добавление мобильного устройства в случае, если общий сертификат доставляется с помощью ссылки App Store

► *Чтобы установить на iOS-устройство приложение Kaspersky Safe Browser из App Store и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства iOS.
2. В окне мастера **Способ управления iOS устройствами** выберите вариант **Установить Kaspersky Safe Browser по ссылке на App Store**.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:
   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

     По умолчанию этот вариант выбран.
   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге было выбрано несколько пользователей.
4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:
   - **Показать ссылку в мастере**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить ссылку пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер

телефона и отредактировать текст отправляемого SMS-сообщения.

Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS-оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на мобильное устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Safe Browser с App Store. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку Kaspersky Safe Browser. Пользователь устанавливает Kaspersky Safe Browser на мобильное устройство. После установки Kaspersky Safe Browser пользователь повторно сканирует QR-код для получения параметров подключения к Серверу администрирования. В результате повторного сканирования QR-кода в Safe Browser пользователь получает параметры подключения к Серверу администрирования и общий сертификат. Мобильное устройство подключается к Серверу администрирования и загружает себе общий сертификат. Сертификат, установленный на мобильное устройство, будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли. Если Kaspersky Safe Browser был установлен ранее на мобильное устройство, параметры подключения к Серверу администрирования нужно вводить самостоятельно. После этого необходимо установить на мобильное устройство общий сертификат (см. раздел "Установка сертификата" на стр. 685). Загрузка и установка Kaspersky Safe Browser в этом случае не выполняется.

Добавление мобильного устройства в случае, если общий сертификат доставляется в составе iOS MDM-профиля

► *Чтобы подключить к Серверу администрирования iOS-устройство по протоколу iOS MDM, выполните следующие действия:*

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **iOS**.
2. В окне мастера **Способ управления iOS устройствами** выберите **Управлять iOS устройствами с помощью iOS MDM-профиля**.

   В появившемся поле ниже выберите Сервер iOS MDM.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

     По умолчанию этот вариант выбран.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ недоступен, если на

предыдущем шаге было выбрано несколько пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать ссылку в мастере**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить ссылку пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

     Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS-оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате iOS MDM-профиль автоматически публикуется на Веб-сервере Kaspersky Security Center. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки iOS MDM-профиля с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку iOS MDM-профиля. Чтобы iOS MDM-профиль загрузился на мобильное устройство, пользователь должен согласиться на установку iOS MDM-профиля. После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Для перехода пользователем по полученной ссылке на Веб-сервере Kaspersky Security Center необходимо, чтобы с его мобильного устройства было доступно соединение с Сервером администрирования по порту 8061.

Добавление мобильного устройства в случае, если общий сертификат доставляется с помощью ссылки Google Play

► *Чтобы установить на KES-устройство приложение Kaspersky Endpoint Security для Android из Google Play и затем подключить устройство к Серверу администрирования, выполните следующие*

действия:

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.
2. В окне мастера **Способ установки Kaspersky Endpoint Security для Android** выберите вариант **По ссылке на Google Play**.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

     По умолчанию этот вариант выбран.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге было выбрано несколько пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать ссылку в мастере**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

   - **Отправить ссылку пользователю**

     При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

     Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

     Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS-оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на мобильное устройство пользователя будет отправлена ссылка и QR-код

для загрузки Kaspersky Endpoint Security для Android. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление мобильного устройства в случае, если общий сертификат доставляется в составе мобильного приложения

► *Чтобы установить на Android-устройство приложение Kaspersky Endpoint Security для Android и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

Для установки используется приложение Kaspersky Endpoint Security для Android, опубликованное на Сервере администрирования.

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.
2. В окне мастера **Способ установки Kaspersky Endpoint Security для Android** выберите вариант **По ссылке на Веб-сервер**.

   В появившемся поле ниже выберите инсталляционный пакет или создайте новый инсталляционный пакет по кнопке **Новый**.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

   - **Выписать сертификат средствами Сервера администрирования**

     Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

     По умолчанию этот вариант выбран.

   - **Указать файл сертификата**

     Укажите файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге было выбрано несколько пользователей.
4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

   - **Показать ссылку в мастере**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

- **Отправить ссылку пользователю**

  При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

  Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

  Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS-оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате пакет мобильного приложения Kaspersky Endpoint Security для Android автоматически публикуется на Веб-сервере Kaspersky Security Center. Пакет мобильного приложения содержит приложение, параметры подключения мобильного устройства к Серверу администрирования и сертификат. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки пакета с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система устройства запрашивает у пользователя согласие на установку пакета мобильного приложения. Если пользователь соглашается, пакет загружается на мобильное устройство. После загрузки пакета и синхронизации с Сервером администрирования мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Управление мобильными устройствами Exchange ActiveSync

В этом разделе описаны дополнительные возможности управления EAS-устройствами с помощью Kaspersky Security Center.

Кроме управления EAS-устройствами с помощью команд, администратор может использовать следующие возможности:

- Создавать профили управления EAS-устройствами, назначать их почтовым ящикам пользователей (см. стр. 700). *Профиль управления EAS-устройствами* – это политика Exchange ActiveSync, которая используется на сервере Microsoft Exchange для управления EAS-устройствами. В профиле управления EAS-устройствами вы можете настраивать следующие группы параметров:
  - параметры управления паролем пользователя;
  - параметры синхронизации почты;
  - ограничения для использования функций мобильного устройства;

- ограничения для использования мобильных приложений на мобильном устройстве.

> В зависимости от модели мобильного устройства параметры профиля управления могут применяться частично. Статус применения политики Exchange ActiveSync вы можете посмотреть в свойствах мобильного устройства.

- Просматривать информацию о параметрах управления EAS-устройствами (см. стр. 703). Например, в свойствах мобильного устройства администратор может посмотреть время последней синхронизации мобильного устройства с сервером Microsoft Exchange, идентификатор EAS-устройства, название политики Exchange ActiveSync и статус ее применения на мобильном устройстве.
- Отключать неиспользуемые пользователями EAS-устройства от управления (см. стр. 704).
- Настраивать параметры опроса Active Directory Сервером мобильных устройств Exchange ActiveSync, в результате которого обновляется информация о почтовых ящиках пользователей и их мобильных устройствах.

В этом разделе

Добавление профиля управления

Для управления EAS-устройствами вы можете создавать профили управления EAS-устройствами и назначать их выбранным почтовым ящикам Microsoft Exchange.

> Почтовому ящику Microsoft Exchange может быть назначен только один профиль управления EAS-устройствами.

► *Чтобы добавить профиль управления EAS-устройствами для почтового ящика Microsoft Exchange, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер мобильных устройств Exchange ActiveSync.
4. В контекстном меню Сервера мобильных устройств Exchange ActiveSync выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.
5. В окне свойств **Сервера мобильных устройств Exchange ActiveSync** выберите раздел **Почтовые ящики**.
6. Выберите почтовый ящик и нажмите на кнопку **Назначить профиль**.

   Откроется окно **Профили политики**.
7. В окне **Профили политики** нажмите на кнопку **Добавить**.

   Откроется окно **Новый профиль**.
8. Выполните настройку параметров профиля на закладках окна **Новый профиль**
   - Если вы хотите задать имя профиля и период его обновления, выберите закладку **Общие**.
   - Если вы хотите настроить параметры пароля пользователя мобильного устройства, выберите закладку **Пароль**.
   - Если вы хотите настроить параметры синхронизации с сервером Microsoft Exchange, выберите закладку **Синхронизация**.
   - Если вы хотите настроить параметры ограничения функций мобильного устройства, выберите закладку **Устройство**.
   - Если вы хотите настроить параметры ограничения использования мобильных приложений на мобильном устройстве, выберите закладку **Ограничения приложений**.
9. Нажмите на кнопку **ОК**.

   Новый профиль отобразится в списке профилей в окне **Профили политики**.

   Если вы хотите, чтобы этот профиль автоматически присваивался новым почтовым ящикам и почтовым ящикам, профиль которых был удален, выберите его в списке профилей и нажмите на кнопку **Сделать профилем по умолчанию**.

   > Профиль по умолчанию нельзя удалить. Чтобы удалить текущий профиль по умолчанию, необходимо назначить свойство "профиль по умолчанию" другому профилю.
10. Нажмите на кнопку **ОК** в окне **Профили политики**.

    Параметры профиля управления будут применены на EAS-устройстве при следующей

синхронизации устройства с Сервером мобильных устройств Exchange ActiveSync.

Удаление профиля управления

► *Чтобы удалить профиль управления EAS-устройствами для почтового ящика Microsoft Exchange, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер мобильных устройств Exchange ActiveSync.
4. В контекстном меню Сервера мобильных устройств Exchange ActiveSync выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.
5. В окне свойств Сервера мобильных устройств Exchange ActiveSync выберите раздел **Почтовые ящики**.
6. Выберите почтовый ящик и нажмите на кнопку **Изменить профили**.

   Откроется окно **Профили политики**.
7. В окне **Профили политики** выберите профиль, который вы хотите удалить, и нажмите на кнопку удаления с красным крестом.

   Выбранный профиль будет удален из списка профилей управления. К EAS-устройствам, находящимся под управлением удаленного профиля, будет применен текущий профиль по умолчанию.

   Если вы хотите удалить текущий профиль по умолчанию, назначьте свойство "профиль по умолчанию" другому профилю, затем удалите профиль.

Работа с политиками Exchange ActiveSync

После установки Сервера мобильных устройств Exchange ActiveSync в разделе **Почтовые ящики** окна свойств этого Сервера вы можете посмотреть информацию об учетных записях сервера Microsoft Exchange, полученных в результате опроса текущего домена либо леса доменов.

Кроме того, в окне свойств Сервера мобильных устройств Exchange ActiveSync вы можете использовать следующие кнопки:

- **Изменить профили** – позволяет открыть окно **Профили политики**, содержащее список политик, полученных с сервера Microsoft Exchange. В этом окне можно создавать, изменять или удалять политики Exchange ActiveSync. Окно **Профили политики** почти полностью соответствует окну редактирования политик в консоли Exchange Management Console.
- **Назначить профили мобильным устройствам** – позволяет назначить выбранную политику Exchange

ActiveSync одной или нескольким учетным записям.

- **Вкл/выкл ActiveSync** – позволяет включить или выключить HTTP протокол Exchange ActiveSync для одной или нескольких учетных записей.

Настройка области сканирования

В свойствах установленного Сервера мобильных устройств Exchange ActiveSync в разделе **Параметры** вы можете настроить область сканирования. По умолчанию область сканирования – это текущий домен, в котором установлен Сервер мобильных устройств Exchange ActiveSync. При выборе значения **Весь лес доменов** область сканирования расширится на весь лес доменов.

Работа с EAS-устройствами

Устройства, полученные в результате сканирования сервера Microsoft Exchange, попадают в единый список устройств, который находится в узле **Управление мобильными устройствами** в папке **Мобильные устройства**.

Если вы хотите, чтобы в папке **Мобильные устройства** отображались только устройства Exchange ActiveSync (далее EAS-устройства), отфильтруйте список устройств по ссылке **Exchange ActiveSync (EAS)**, расположенной над ним.

Вы можете управлять EAS-устройствами с помощью команд. Например, команда **Сбросить настройки до заводских** позволяет удалить все данные с устройства и сбросить настройки устройства до заводских. Эта команда полезна в случае кражи или потери устройства, когда необходимо избежать попадания корпоративных или персональных данных к третьим лицам.

Если с устройства были удалены все данные, то при следующем подключении этого устройства к серверу Microsoft Exchange с него снова будут удалены все данные. Команда будет повторяться до тех пор, пока устройство не будет удалено из списка устройств. Такое поведение обусловлено особенностями работы сервера Microsoft Exchange.

Чтобы удалить EAS-устройство из списка, в контекстном меню устройства выберите пункт **Удалить**. Если с EAS-устройства не будет удалена учетная запись Exchange ActiveSync, то при последующей синхронизации устройства с сервером Microsoft Exchange оно снова появится в списке устройств.

Просмотр информации о EAS-устройстве

► *Чтобы просмотреть информацию о EAS-устройстве, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте EAS-устройства по типу протокола управления (**EAS**).

3. В контекстном меню мобильного устройства выберите пункт **Свойства**.

   В результате откроется окно свойств EAS-устройства.

В окне свойств мобильного устройства отображается информация о подключенном EAS-устройстве.

Отключение EAS-устройства от управления

► *Чтобы отключить EAS-устройство от управления Сервером мобильных устройств Exchange ActiveSync, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте EAS-устройства по типу протокола управления (**EAS**).
3. Выберите мобильное устройство, которое вы хотите отключить от управления Сервером мобильных устройств Exchange ActiveSync.
4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате EAS-устройство будет отмечено на удаление значком с красным крестом. Фактическое удаление мобильного устройства из списка управляемых устройств произойдет после его удаления из базы данных Сервера мобильных устройств Exchange ActiveSync. Для этого администратору необходимо удалить учетную запись пользователя на сервере Microsoft Exchange.

Права пользователя для управления мобильными устройствами Exchange ActiveSync

Для управления мобильными устройствами, которые работают по протоколу Exchange ActiveSync с сервером Microsoft Exchange Server 2010 или Microsoft Exchange Server 2013, необходимо, чтобы пользователь был членом ролевой группы, для которой разрешены выполнения следующих командлетов:

- Get-CASMailbox;
- Set-CASMailbox;
- Remove-ActiveSyncDevice;
- Clear-ActiveSyncDevice;
- Get-ActiveSyncDeviceStatistics;
- Get-AcceptedDomain;
- Set-AdServerSettings;
- Get-ActiveSyncMailboxPolicy;
- New-ActiveSyncMailboxPolicy;
- Set-ActiveSyncMailboxPolicy;

- Remove-ActiveSyncMailboxPolicy.

Для управления мобильными устройствами, которые работают по протоколу Exchange ActiveSync с сервером Microsoft Exchange Server 2007, необходимо, чтобы пользователь обладал административными правами. В случае их отсутствия выполните командлеты для наделения административными правами пользователя (см. таблицу ниже).

Таблица 62. Административные права для управления мобильными устройствами Exchange ActiveSync для Microsoft Exchange Server 2007

Доступ	Объект	Командлет
Полный	Ветка "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`
Чтение	Ветка "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll`
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	`Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Имя домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Полный	Хранилища почтовых ящиков ms-Exch-Store-Admin для mailboxstorages	`Get-MailboxDatabase | Add-ADPermission -User <имя пользователя или группы> -ExtendedRights ms-Exch-Store-Admin`

Подробную информацию об использовании командлетов в консоли Exchange Management Shell смотрите на веб-сайте технической поддержки Microsoft Exchange Server http://technet.microsoft.com/ru-ru/library/bb123778(v=exchg.150).aspx.

Управление iOS MDM-устройствами

В этом разделе описаны дополнительные возможности управления iOS MDM-устройствами с помощью Kaspersky Security Center. Для управления iOS MDM-устройствами программа поддерживает следующие возможности:

- Централизованно настраивать параметры управляемых iOS MDM-устройств и ограничивать функции устройств с помощью конфигурационных профилей. Вы можете добавлять и изменять конфигурационные профили и устанавливать профили на мобильные устройства.
- Устанавливать приложения на мобильные устройства не через App Store с помощью provisioning-профилей. Например, с помощью provisioning-профилей можно устанавливать на мобильные устройства пользователей корпоративные приложения, разработанные внутри компании. Provisioning-профиль содержит информацию о приложении и мобильном устройстве.
- Устанавливать приложения на iOS MDM-устройство через App Store. Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM.

Каждые 24 часа всем подключенным iOS MDM-устройствам отправляется PUSH-нотификация для синхронизации данных с Сервером iOS MDM (см. раздел "Установка Сервера iOS MDM" на стр. 155).

Информацию о конфигурационном профиле и provisioning–профиле, а также о приложениях, установленных на iOS MDM-устройстве, можно просмотреть в окне свойств устройства (см. раздел "Просмотр информации о iOS MDM-устройстве" на стр. 717).

В этом разделе

Выписка сертификата iOS MDM-профиля

Вы можете выписать сертификат iOS MDM-профиля для определения его подлинности мобильным устройством.

► *Чтобы создать сертификат iOS MDM-профиля, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры подключения iOS-устройств**.
4. Нажмите на кнопку **Задать** ниже поля **Выберите сертификат**.

   В результате откроется окно **Сертификат**.
5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:
   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.

- Если выбрано значение **X.509-сертификат**:
  a. укажите файл закрытого ключа (файл с расширением prk или pem);
  b. укажите пароль закрытого ключа;
  c. укажите файл открытого ключа (файл с расширением cer).

6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат iOS MDM-профиля.

Добавление конфигурационного профиля

Для создания конфигурационного профиля необходимо установить программу iPhone Configuration Utility на том же устройстве, на котором установлена Консоль администрирования. Программу iPhone Configuration Utility нужно предварительно скачать с сайта Apple Inc. и установить штатными средствами операционной системы.

► *Чтобы создать конфигурационный профиль и добавить его на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

   Папка **Управление мобильными устройствами** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области папки **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств Сервера iOS MDM выберите раздел **Конфигурационные профили**.
6. В разделе **Конфигурационные профили** нажмите на кнопку **Создать**.

   Откроется окно **Добавление нового конфигурационного профиля**.

7. В окне **Добавление нового конфигурационного профиля** укажите название профиля и идентификатор профиля.

   Идентификатор конфигурационного профиля должен быть уникальным, значение идентификатора следует задавать в формате Reverse-DNS, например, *com.companyname.identifier*.

8. Нажмите на кнопку **ОК**.

   Запустится программа iPhone Configuration Utility.

9. Выполните настройку параметров профиля в программе iPhone Configuration Utility.

   Описание параметров профиля и инструкции по его настройке приведены в документации для

программы iPhone Configuration Utility.

После настройки параметров профиля в программе iPhone Configuration Utility, новый конфигурационный профиль отображается в разделе **Конфигурационные профили** в окне свойств Сервера iOS MDM.

По кнопке **Изменить** конфигурационный профиль можно отредактировать.

По кнопке **Импортировать** можно загрузить конфигурационный профиль в программу.

По кнопке **Экспортировать** конфигурационный профиль можно сохранить в файле.

Созданный профиль требуется установить на iOS MDM-устройства (см. раздел "Установка конфигурационного профиля на устройство" на стр. 709).

Установка конфигурационного профиля на устройство

► *Чтобы установить конфигурационный профиль на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, на которое нужно установить конфигурационный профиль

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить профиль**.

   В результате откроется окно **Выбор профилей** со списком профилей. Выберите в списке профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Выполнено*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя

еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Установленный профиль можно просмотреть и при необходимости удалить (см. раздел "Удаление конфигурационного профиля с устройства" на стр. 710).

Удаление конфигурационного профиля с устройства

► *Чтобы удалить конфигурационный профиль с мобильного устройства, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.
3. Выберите мобильное устройство пользователя, с которого нужно удалить конфигурационный профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить профиль**.

   В результате откроется окно **Удаление профилей** со списком профилей.

6. Выберите в списке профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.
7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный конфигурационный профиль будет удален с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда

еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление нового устройства посредством публикации ссылки на профиль

В Консоли администрирования с помощью мастера подключения нового мобильного устройства администратор создает новый iOS MDM-профиль. В результате работы мастера будут выполнены следующие действия:

- iOS MDM-профиль автоматически опубликуется на веб-сервере.
- Пользователю будет отправлена ссылка на iOS MDM-профиль в SMS-сообщении или по электронной почте. После получения ссылки пользователь установит iOS MDM-профиль на мобильном устройстве.
- В результате мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

См. также:

Веб-сервер Kaspersky Security Center 176

Добавление нового устройства посредством установки профиля администратором

Чтобы подключить мобильное устройство к Серверу iOS MDM с помощью установки iOS MDM-профиля на мобильное устройство, администратор должен выполнить следующие действия:

1. В Консоли администрирования открыть мастер подключения нового устройства.
2. Создать новый iOS MDM-профиль, установив в окне мастера создания профиля флажок **Показать сертификат после завершения работы мастера**.
3. Сохранить iOS MDM-профиль.
4. Установить iOS MDM-профиль на мобильное устройство пользователя с помощью утилиты Apple Configurator.

В результате мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

См. также:

Веб-сервер Kaspersky Security Center 176

Добавление provisioning-профиля

► *Чтобы добавить provisioning-профиль на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера мобильных устройств.
5. В окне свойств **Сервера iOS MDM** перейдите в раздел **Provisioning-профили**.
6. В разделе **Provisioning-профили** нажмите на кнопку **Импортировать** и укажите путь к файлу provisioning-профиля.

Профиль будет добавлен в параметры Сервера iOS MDM.

По кнопке **Экспортировать** provisioning-профиль можно сохранить в файле.

Импортированный provisioning-профиль можно установить на iOS MDM-устройства (см. раздел "Установка provisioning-профиля на устройство" на стр. 712).

Установка provisioning-профиля на устройство

► *Чтобы установить provisioning-профиль на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.
3. Выберите мобильное устройство пользователя, на которое нужно установить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них provisioning-профиль

одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить provisioning-профиль**.

   В результате откроется окно **Выбор provisioning-профилей** со списком provisioning-профилей. Выберите в списке provisioning-профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.
6. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.
7. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Установленный профиль можно просмотреть и при необходимости удалить (см. раздел "Удаление provisioning-профиля с устройства" на стр. 713).

Удаление provisioning-профиля с устройства

► *Чтобы удалить provisioning-профиль с мобильного устройства, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.
3. Выберите мобильное устройство пользователя, с которого нужно удалить provisioning-профиль.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них provisioning-профиль одновременно.
4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить**

provisioning-профиль и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить provisioning-профиль**.

В результате откроется окно **Удаление provisioning-профилей** со списком профилей.

6. Выберите в списке provisioning-профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.
7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранный provisioning-профиль будет удален с мобильного устройства пользователя. Приложения, связанные с удаленным provisioning-профилем, не будут работать. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

   В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.
8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление управляемого приложения

Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM. Приложение является управляемым, если оно было установлено на устройство с помощью Kaspersky Security Center. Управляемым приложением можно дистанционно управлять средствами Kaspersky Security Center.

► *Чтобы добавить управляемое приложение на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

   Откроется окно свойств Сервера iOS MDM.
5. В окне свойств Сервера iOS MDM выберите раздел **Управляемые приложения**.
6. В разделе **Управляемые приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление приложения**.

7. В окне **Добавление приложения** в поле **Название приложения** укажите название добавляемого приложения.
8. В поле **Apple ID приложения или ссылка на приложение в App Store** укажите Apple ID добавляемого приложения или ссылку на манифест-файл, по которой можно загрузить приложение.
9. Если вы хотите, чтобы при удалении iOS MDM-профиля одновременно с профилем с мобильного устройства пользователя было удалено и управляемое приложение, установите флажок **Удалять вместе с iOS MDM-профилем**.
10. Если вы хотите запретить резервное копирование данных приложения с помощью iTunes, установите флажок **Запретить создавать резервные копии данных**.
11. Нажмите на кнопку **ОК**.

Добавленное приложение отображается в разделе **Управляемые приложения** окна свойств Сервера iOS MDM.

Установка приложения на мобильное устройство

► *Чтобы установить приложение на мобильное устройство iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. Выберите iOS MDM-устройство, на которое нужно установить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы установить на них приложение одновременно.
3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
4. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить приложение**.

   В результате откроется окно **Выбор приложений** со списком приложений. Выберите в списке приложение, которое нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.
5. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет установлено на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершена*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз. По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

6. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Информация об установленном приложении отображается в свойствах мобильного устройства iOS MDM (см. раздел "Просмотр информации о iOS MDM-устройстве" на стр. 717). Вы можете удалить приложение с мобильного устройства с помощью журнала команд или из контекстного меню мобильного устройства (см. раздел "Удаление приложения с устройства" на стр. 716).

Удаление приложения с устройства

► *Чтобы удалить приложение с мобильного устройства, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.
3. Выберите мобильное устройство пользователя, с которого нужно удалить приложение.

   Вы можете выбрать несколько мобильных устройств, чтобы удалить с них приложение одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить приложение** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Удалить приложение**.

   В результате откроется окно **Удаление приложений** со списком приложений.

6. Выберите в списке приложение, которое нужно удалить с мобильного устройства. Вы можете выбрать и удалить с устройства несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.
7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

   В результате выполнения команды выбранное приложение будет удалено с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершена*.

   По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

   По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда

еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Настройка параметров роуминга на мобильном устройстве iOS MDM

► *Чтобы настроить параметры роуминга, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
3. Выберите iOS MDM-устройство пользователя, для которого нужно настроить роуминг.

   Вы можете выбрать несколько мобильных устройств, чтобы настроить для них роуминг одновременно.
4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Настроить параметры роуминга** и нажмите на кнопку **Отправить команду**.

   Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды** → **Настроить параметры роуминга**.
6. В окне **Параметры роуминга** укажите нужные вам параметры:

   - **Включить голосовой роуминг**

     Если флажок установлен, на мобильном устройстве iOS MDM включен голосовой роуминг. Пользователь iOS MDM-устройства может звонить и отвечать на звонки в роуминге.

     По умолчанию флажок установлен.

   - **Включить роуминг данных**

Если флажок установлен, на мобильном устройстве iOS MDM включен роуминг данных. Пользователь iOS MDM-устройства может пользоваться интернетом в роуминге.

По умолчанию флажок снят.

Параметры роуминга будут настроены для выбранных устройств.

Просмотр информации о iOS MDM-устройстве

► *Чтобы просмотреть информацию о iOS MDM-устройстве, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку

Мобильные устройства.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.
3. Выберите мобильное устройство, информацию о котором нужно просмотреть.
4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

   В результате откроется окно свойств iOS MDM-устройства.

В окне свойств мобильного устройства отображается информация о подключенном iOS MDM-устройстве.

Отключение iOS MDM-устройства от управления

► *Чтобы отключить iOS MDM-устройство от Сервера iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.
3. Выберите мобильное устройство, которое необходимо отключить.
4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

   В результате iOS MDM-устройство будет отмечено в списке на удаление. Мобильное устройство будет автоматически удалено из списка управляемых устройств после его удаления из базы данных Сервера iOS MDM. Удаление мобильного устройства из базы данных Сервера iOS MDM происходит в течение одной минуты.

В результате отключения iOS MDM-устройства от управления с мобильного устройства будут удалены все установленные конфигурационные профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем** (см. раздел "**Добавление управляемого приложения**" на стр. 714) .

Отправка команд на устройство

► *Чтобы отправить команду на iOS MDM-устройство, администратор должен выполнить следующие действия:*

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать мобильное устройство, на которое необходимо отправить команды.
4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. Во всплывающем списке выберите необходимую команду для отправки на мобильное устройство.

Проверка статуса исполнения отправленных команд

► *Чтобы проверить статус выполнения отправленной команды на мобильном устройстве, администратор должен выполнить следующие действия:*

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать мобильное устройство, на котором необходимо проверить статус выполнения отправленных команд.
4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

Управление KES-устройствами

Kaspersky Security Center поддерживает следующие возможности для управления мобильными KES-устройствами:

- централизованно управлять KES-устройствами с помощью команд (см. раздел "Команды для управления мобильным устройством" на стр. 679);
- просматривать информацию о параметрах управления KES-устройствами (см. раздел "Просмотр информации о KES-устройстве" на стр. 721);
- устанавливать приложения с помощью пакетов мобильных приложений (см. раздел "Создание пакета мобильных приложений для KES-устройств" на стр. 719);
- отключать KES-устройства от управления (см. раздел "Отключение KES-устройства от управления" на стр. 721).

В этом разделе

Создание пакета мобильных приложений для KES-устройств

Для создания пакета мобильных приложений для KES-устройств необходима лицензия Kaspersky Endpoint Security для Android.

► *Чтобы создать пакет мобильных приложений, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Дополнительные действия** и из раскрывающегося списка выберите пункт **Управлять пакетами мобильных приложений**.
3. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Новый**.
4. Запустится мастер создания пакета мобильных приложений. Следуйте далее указаниям мастера.
5. Если вы хотите поместить программу в контейнер, в окне мастера **Параметры** установите флажок **Создать контейнер с выбранным приложением**.

   Если на рабочем месте администратора установлен плагин Kaspersky Endpoint Security для Android Service Pack 3 Maintenance Release 2 или более поздней версии, флажок **Создать контейнер с выбранным приложением** недоступен. Поддержка создания контейнеров для мобильных приложений прекращена. Вы можете доставлять на Android-устройства контейнеры, созданные в более ранних версиях.

Созданный пакет мобильных приложений отобразится в окне **Управление пакетами мобильных приложений**.

Контейнеры используются для контроля активности программ, запускаемых на мобильном устройстве пользователя. К программам, помещенным в контейнер, могут быть применены правила политики безопасности. Правила для программ можно настроить в окне свойств политики программы Kaspersky Endpoint Security для Android в разделе **Контейнеры**. Подробная информация о контейнерах и работе с ними приведена в документации для программы Kaspersky Endpoint Security для Android.
Вы можете поместить в контейнер стороннюю программу. Невозможно поместить в контейнер дистрибутив Kaspersky Endpoint Security 10 для Android.

Включение двухфакторной аутентификации KES-устройств

► *Чтобы включить двухфакторную аутентификацию KES-устройства, выполните следующие действия:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM
   - для 32-разрядной системы:

     HKLM\Software\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Создайте ключ с именем LP_MobileMustUseTwoWayAuthOnPort13292.

4. Укажите тип ключа REG_DWORD.
5. Установите значение ключа 1.
6. Перезапустите службу Сервера администрирования.

В результате обязательная двухфакторная аутентификация KES-устройства с использованием общего сертификата будет включена после запуска службы Сервера администрирования.

> При первом подключении KES-устройства к Серверу администрирования наличие сертификата не обязательно.

По умолчанию двухфакторная аутентификация KES-устройств отключена.

Просмотр информации о KES-устройстве

► *Чтобы просмотреть информацию о KES-устройстве, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.
3. Выберите мобильное устройство, информацию которого нужно просмотреть.
4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств KES-устройства.

В окне свойств мобильного устройства отображается информация о подключенном KES-устройстве.

Отключение KES-устройства от управления

Чтобы отключить KES-устройство от управления, пользователь должен удалить Агент администрирования с мобильного устройства. После удаления пользователем Агента администрирования информация о мобильном устройстве удаляется из базы данных Сервера администрирования и администратор может удалить мобильное устройство из списка управляемых устройств.

► *Чтобы удалить KES-устройство из списка управляемых устройств, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.
2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.
3. Выберите мобильное устройство, которое необходимо отключить от управления.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате мобильное устройство будет удалено из списка управляемых устройств.

Если Kaspersky Endpoint Security для Android не удален с мобильного устройства, то после синхронизации с Сервером администрирования мобильное устройство снова появится в списке управляемых устройств.

Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

Данные, которые используются для отслеживания состояния устройств и их обслуживания, отображаются в папке дерева консоли **Хранилища**.

Папка **Хранилища** содержит следующие объекты:

- полученные Сервером администрирования обновления, которые распространяются на клиентские устройства (см. раздел "Просмотр полученных обновлений" на стр. 376);
- список оборудования, обнаруженного в сети;
- ключи, обнаруженные на клиентских устройствах (см. раздел "Программы "Лаборатории Касперского": лицензирование и активация" на стр. 295);
- файлы, помещенные программами безопасности в карантинные папки на устройствах;
- файлы, помещенные в резервные хранилища устройств;
- файлы, для которых программы безопасности определили необходимость отложенной проверки.

В этом разделе

Экспорт списка объектов, находящихся в хранилище, в текстовый файл

Вы можете экспортировать в текстовый файл список объектов, находящихся в хранилище.

► *Чтобы экспортировать в текстовый файл список объектов, находящихся в хранилище, выполните*

следующие действия:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку нужного вам хранилища.
2. В контекстном меню списка объектов хранилища выберите пункт **Экспортировать список**.

   В результате откроется окно **Экспорт списка**, в котором вы можете указать имя текстового файла и адрес папки, в которую он будет помещен.

Инсталляционные пакеты

Kaspersky Security Center помещает в хранилища данных инсталляционные пакеты программ "Лаборатории Касперского" и программ сторонних производителей.

Инсталляционный пакет представляет собой набор файлов, необходимых для установки программы. Инсталляционный пакет содержит параметры процесса установки и первоначальной конфигурации устанавливаемой программы.

Если вы хотите установить какую-либо программу на клиентское устройство, для этой программы необходимо создать инсталляционный пакет для этой программы (см. раздел "Создание инсталляционных пакетов программ" на стр. 670), или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

См. также:

Работа с инсталляционными пакетами 284

Основные статусы файлов в хранилище

Программы безопасности проверяют файлы на устройствах на наличие известных вирусов и других программ, представляющих угрозу, присваивают статусы файлам и помещают некоторые файлы в хранилище.

Например, программы безопасности могут

- сохранять в хранилище копию файла перед удалением;
- изолировать в хранилище возможно зараженные файлы.

Основные статусы файлов приведены в таблице ниже. Вы можете получить более подробную информацию о действиях с файлами в справках программ безопасности.

Таблица 63. Статусы файлов в хранилище

Название статуса	Описание статуса

Название статуса	Описание статуса
Заражен	В файле найден участок кода известного вируса или другой представляющей угрозу программы, информация о которой содержится в антивирусных базах "Лаборатории Касперского".
Не заражен	В файле не обнаружено известных вирусов или других программ, представляющих угрозу.
Предупреждение	В файле содержится участок кода, частично совпадающий с контрольным участком кода известной угрозы.
Возможно зараженный	В файле содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, пока не известный "Лаборатории Касперского".
Помещен в папку пользователем	Пользователь самостоятельно поместил файл в хранилище, например, поведение файла давало основание подозревать в нем наличие угрозы. Пользователь может проверить файл на наличие в нем угроз с помощью обновленных баз.
Ложное срабатывание	Программа "Лаборатории Касперского" присвоила статус незараженному файлу как зараженному ввиду того, что его код напоминает код вируса. После проверки с применением обновленных баз файл определяется как незараженный.
Вылечен	Файл удалось вылечить.
Удален	Файл удален в результате обработки.
Защищен паролем	Файл не может быть обработан по причине того, что он защищен паролем.

См. также:

Значки статусов файлов в Консоли администрирования.....864

Срабатывание правил в обучающем режиме

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в обучающем режиме, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky Security Center. Эта информация хранится в виде списка в папке **Срабатывание правил в интеллектуальном режиме**, которая вложена в папку **Хранилища**. Вы можете подтвердить обнаружение как корректное (см. раздел "Просмотр списка

обнаружений, выполненных с помощью правил Адаптивного контроля аномалий" на стр. 725) или добавить его в исключения (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. 727).

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security.

В этом разделе

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

► *Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий, выполните следующие действия:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в обучающем режиме** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя.**

     Имя правила, которое было применено.

   - **Состояние**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации

обнаружение пропадет из списка.

Пусто – если администратор не обработал обнаружение.

- **Всего срабатываний правил**

  Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя.**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA-256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA-256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA-256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA-256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

► *Чтобы просмотреть свойства каждого элемента, выполните следующие действия:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в обучающем режиме** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области папки **Срабатывание правил в обучающем режиме** выберите требуемый объект.
4. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
   - В контекстном меню объекта выберите пункт **Свойства**.

   В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий (см. раздел "Срабатывание правил в интеллектуальном режиме" на стр. 724) .

► *Чтобы подтвердить объект,*

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждается**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

► *Чтобы добавить объект в исключения,*

в списке обнаруженных объектов в контекстном меню одного или нескольких объектов выберите пункт **Добавить в исключения**.

Запустится мастер добавления исключений (см. раздел "Добавление исключений в правила Адаптивного контроля аномалий" на стр. 727). Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

► *Чтобы запустить мастер добавления исключений с помощью списка адаптивного обнаружения аномалий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в обучающем режиме** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

В результате запустится мастер добавления устройств.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте закладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений**.

В этом разделе

Шаг 1. Выбор программы

Этот шаг можно пропустить, если у вас есть только программа Kaspersky Endpoint Security для Windows и нет других программ, поддерживающих правила адаптивного контроля аномалий.

Мастер добавления исключений отображает список программ "Лаборатории Касперского", для которых плагины управления позволяют добавлять исключения к политикам для этих программ. Выберите программу из списка и нажмите на кнопку **Далее**, чтобы продолжить выбор политики, для которой будет добавлено исключение.

Шаг 2. Выбор политики (политик)

Мастер отображает список политик (с профилями политик) для Kaspersky Endpoint Security.

Выберите все политики и профили политик, в которые вы хотите добавить исключения, и нажмите на кнопку **Далее**.

Шаг 3. Обработка политики (политик)

Мастер отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

Это последний шаг мастера. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Карантин и резервное хранилище

Антивирусные программы "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы на карантин или в резервное хранилище.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Резервное хранилище предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center формирует общий список файлов, помещенных на карантин и в резервное хранилище программами "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах на карантине и в резервных хранилищах на Сервер администрирования. Через Консоль администрирования можно просматривать свойства файлов, находящихся в хранилищах на устройствах, запускать антивирусную проверку хранилищ и удалять из них файлы. Значки статусов файлов описаны в приложении (см. раздел "Значки статусов файлов в Консоли администрирования" на стр. 864).

Работа с карантином и резервным хранилищем доступна для Антивируса Касперского для Windows Workstations и Антивируса Касперского для Windows Servers версий 6.0 и выше, а также для Kaspersky Endpoint Security 10 для Windows и выше.

Kaspersky Security Center не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах. Восстановление файлов выполняется на устройстве, где

установлена программа безопасности, поместившая файл в хранилище.

В этом разделе

Включение удаленного управления файлами в хранилищах

По умолчанию удаленное управление файлами в хранилищах на клиентских устройствах отключено.

► *Чтобы включить удаленное управление файлами в хранилищах на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить удаленное управление файлами хранилищ.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику программы безопасности, помещающей файлы в хранилища на устройствах.
4. В окне свойств политики в блоке **Информировать Сервер администрирования** установите флажки, соответствующие хранилищам, для которых вы хотите включить удаленное управление.

   Расположение блока **Информировать Сервер администрирования** в окне свойств политики и названия флажков в блоке индивидуальны для каждой программы безопасности.

Просмотр свойств файла, помещенного в хранилище

► *Чтобы просмотреть свойства файла, помещенного на карантин или в резервное хранилище, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, параметры которого требуется просмотреть.
3. В контекстном меню файла выберите пункт **Свойства**.

Удаление файлов из хранилища

► *Чтобы удалить файл, помещенный на карантин или в резервное хранилище, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Удалить**.
   - По ссылке **Удалить объекты** (**Удалить объект** при удалении одного файла) в блоке работы с выбранными файлами.

В результате программы безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удалят файлы из этих хранилищ.

Восстановление файлов из хранилища

► *Чтобы восстановить файл из карантина или резервного хранилища, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется восстановить.
3. Запустите процесс восстановления файлов одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Восстановить**.
   - По ссылке **Восстановить** в блоке работы с выбранными файлами.

В результате программы безопасности, поместившие файлы в хранилища на клиентских устройствах, восстановят файлы в исходные папки.

Сохранение файла из хранилища на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов, помещенных программой безопасности на карантин или в резервное хранилище на клиентском устройстве. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.

2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, который требуется скопировать на жесткий диск.
3. Запустите процесс копирования файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - По ссылке **Сохранить на диск** в блоке работы с выбранным файлом.

В результате программа безопасности, поместившая файл на карантин на устройстве, сохранит копию файла в указанную папку.

Сканирование файлов, находящихся на карантине

► *Чтобы проверить файлы, находящиеся на карантине, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин**.
2. В рабочей области папки **Карантин** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется проверить.
3. Запустите процесс проверки файлов одним из следующих способов:
   - В контекстном меню файла выберите пункт **Проверить**.
   - По ссылке **Проверить** в блоке работы с выбранными файлами.

   Приложение запускает задачу проверки по требованию для приложений безопасности, которые поместили выбранные файлы на карантин, на устройствах, где хранятся эти файлы.

Необработанные файлы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **Необработанные файлы**.

Отложенная обработка и дезинфекция выполняются программой безопасности по запросу или после определенного события. Вы можете настраивать параметры отложенного лечения файлов.

В этом разделе

Дезинфекция необработанного файла

► *Чтобы запустить лечение необработанного файла, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** выберите файл, который требуется вылечить.
3. Запустите процесс лечения файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Лечить**.
   - По ссылке **Лечить** в блоке работы с выбранным файлом.

   В результате выполняется попытка лечения файла.

Если файл вылечен, программа безопасности, установленная на устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Необработанные файлы**. Если лечение файла невозможно, программа безопасности, установленная на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Необработанные файлы**.

Сохранение необработанного файла на диск

Kaspersky Security Center позволяет сохранять на диск копии необработанных файлов, обнаруженные на клиентских устройствах. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию необработанного файла на диск, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** выберите файлы, которые требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - По ссылке **Сохранить на диск** в блоке работы с выбранным файлом.

В результате программа безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, сохранит копию файла в указанную папку.

Удаление файлов из папки "Необработанные файлы"

► *Чтобы удалить файл из папки **Необработанные файлы**, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:

- В контекстном меню файлов выберите пункт **Удалить**.
- По ссылке **Удалить объекты** (**Удалить объект** при удалении одного файла) в блоке работы с выбранными файлами.

В результате программы безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Необработанные файлы**.

Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

В этом разделе

О KSN и KPSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о программах, установленных на клиентских устройствах.

Участвуя в KSN, вы в соответствии с Положением о KSN соглашаетесь в автоматическом режиме передавать в "Лабораторию Касперского" информацию о работе программ "Лаборатории Касперского", установленных на клиентских устройствах под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN (см. раздел "Настройка доступа к KPSN" на стр. 736).

Программа предлагает присоединиться к KSN во время установки программы и во время работы Мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. раздел "Включение и отключение KPSN" на стр. 738).

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Необходимо использовать Kaspersky Private Security Network или отказаться от использования KSN.

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети

организации.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет программам "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику и файлы в "Лабораторию Касперского". Для получения подробной информации см. *"Kaspersky Private Security Network. Подготовительные процедуры и руководство по эксплуатации*".

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Клиентские устройства, находящиеся под управлением Сервера администрирования, для взаимодействия с KSN или KPSN могут использовать службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет и серверам KPSN.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. 736).

Настройка доступа к KPSN

► *Чтобы настроить доступ Сервера администрирования к KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы включить службу прокси-сервера KPSN.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на

клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

5. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**.
6. Установите флажок **Настроить Локальный KSN** и по кнопке **Выбрать файл с параметрами KSN** загрузите параметры Локального KSN (файлы с расширениями pkcs7, pem).

   Работу с Локальным KSN поддерживают не все программы "Лаборатории Касперского". Подробная информация приводится в Руководствах к соответствующим программам "Лаборатории Касперского".

   > Если для работы с Локальным KSN вы используете версии программ ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование Локального KSN.

7. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:
   - В поле ввода **TCP-порт** укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KPSN. По умолчанию подключение к прокси-серверу KPSN выполняется через порт 13111.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию флажок снят, подключение к прокси-серверу KSN выполняется через UDP-порт 15111.
8. Установите флажок **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

   Если флажок установлен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KPSN. Если флажок снят, подчиненные Серверы администрирования подключаются к KPSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   > Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также установлен флажок **Использовать Сервер администрирования как прокси-сервер**.

9. Нажмите на кнопку **ОК**.

В результате параметры доступа к KPSN будут сохранены.

Включение и отключение KPSN

► *Чтобы включить KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Настроить Локальный KSN**.
5. Нажмите на кнопку **Выбрать файл с параметрами KSN** загрузите параметры Локального KSN (файлы с расширениями pkcs7, pem).

   В результате KPSN будет включен.
6. Нажмите на кнопку **ОК**.

► *Чтобы выключить KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Настроить Локальный KSN**.

   В результате KPSN будет выключен.
5. Нажмите на кнопку **ОК**.

Просмотр статистики прокси-сервера KSN

Прокси-сервер KSN – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и клиентскими устройствами, находящимися под управлением Сервера администрирования.

Использование прокси-сервера KSN предоставляет вам следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

В окне свойств Сервера администрирования вы можете настроить параметры прокси-сервера KSN и просмотреть статистическую информацию об использовании прокси-сервера KSN.

► *Чтобы просмотреть статистику работы прокси-сервера KSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно просмотреть статистику KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Статистика прокси-сервера KSN**.

   В разделе отображается статистика работы прокси-сервера KSN. Если необходимо, выполните дополнительные действия:

   - по кнопке **Обновить** обновите статистическую информацию об использовании прокси-сервера KSN;
   - по кнопке **Экспортировать в файл** экспортируйте данные статистики в файл формата CSV;
   - по кнопке **Проверить подключение к KSN** проверьте, подключен ли Сервер администрирования к KSN в настоящий момент.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Дополнительная защита с использованием Kaspersky Security Network

"Лаборатория Касперского" предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков "Лаборатории Касперского" обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте "Лаборатории Касперского".

Экспорт событий в SIEM-системы

В этом разделе описана процедура экспорта событий, зарегистрированных в Kaspersky Security Center, во внешние системы управления событиями информационной безопасности (SIEM-системы, Security Information and Event Management).

Об экспорте событий

Экспорт событий можно использовать в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

См. также:

Типы событий 495

В этом разделе

События в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования, управляемых устройств и других программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Вы можете экспортировать эту информацию во внешние SIEM-системы. Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

Каждая программа "Лаборатории Касперского" имеет собственный набор событий. *Общие события* – это события, которые произошли на Сервере администрирования или в Агенте администрирования Kaspersky Security Center.

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на потенциально возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

См. также:

Типы событий 495

Процедура экспорта событий

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center, и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Консоли администрирования Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в программах "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий по протоколу Syslog можно выбирать, какие именно события будут переданы в SIEM-систему. Протокол Syslog – это стандартный протокол регистрации сообщений. Поэтому вы можете использовать протокол Syslog для экспорта событий в любую SIEM-систему.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

  Протоколы CEF и LEEF можно использовать для экспорта общих событий, т. е. событий, произошедших на Сервере администрирования или в Агенте администрирования Kaspersky Security Center. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

  > Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного ключа (см. раздел "Программы "Лаборатории Касперского": лицензирование и активация" на стр. 295).

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

См. также:

Особенности лицензирования Kaspersky Security Center и управляемых программ 267

Настройка экспорта событий в Kaspersky Security Center

Для успешного экспорта событий необходимо выполнить настройку в Консоли администрирования Kaspersky Security Center. Настройка Kaspersky Security Center зависит от того, какой способ передачи событий из Kaspersky Security Center в SIEM-систему вы выбрали.

В следующих разделах описано, как настроить Kaspersky Security Center, если вы выбрали экспортировать события следующими способами:

- по протоколу Syslog (см. раздел "Экспорт событий по протоколу Syslog" на стр. 744);
- по протоколам CEF и LEEF (см. раздел "Экспорт событий по протоколам CEF и LEEF" на стр. 755);
- напрямую из базы данных Kaspersky Security Center (см. раздел "Экспорт событий напрямую из базы данных" на стр. 760). (В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm (http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip).)

Экспорт событий по протоколу Syslog

По протоколу Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Протокол Syslog определяется документами "Рабочее предложение" (Request for Comments, RFC), опубликованными Инженерным советом Интернета (Internet Engineering Task Force). Стандарт RFC 5424 (https://tools.ietf.org/html/rfc5424) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы по протоколу Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

В этом разделе

Предварительные условия

При настройке автоматического экспорта событий в Консоли администрирования Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

  Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

Включение автоматического экспорта

Первый шаг настройки экспорта событий по протоколу Syslog – это включение автоматического экспорта в

Kaspersky Security Center.

► *Чтобы включить автоматический экспорт событий по протоколу Syslog, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.
3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

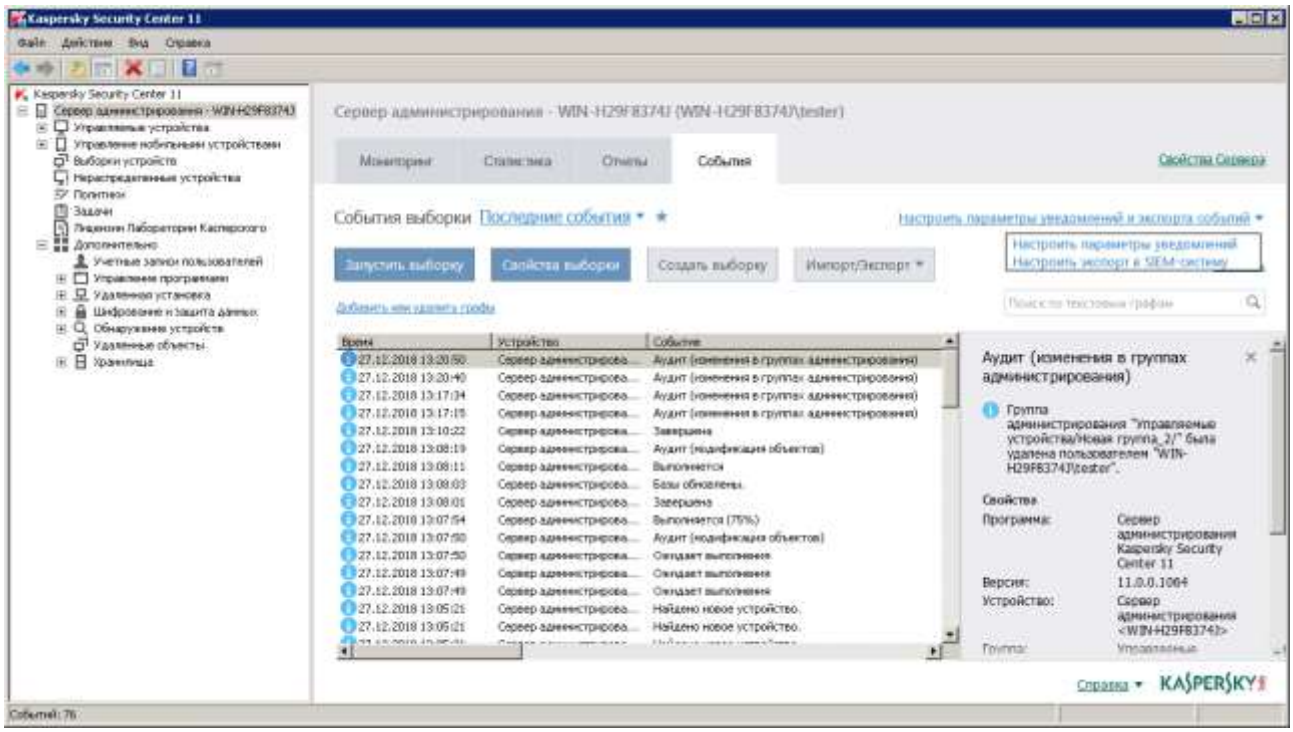


Рисунок 6: Окно свойств событий

Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры:

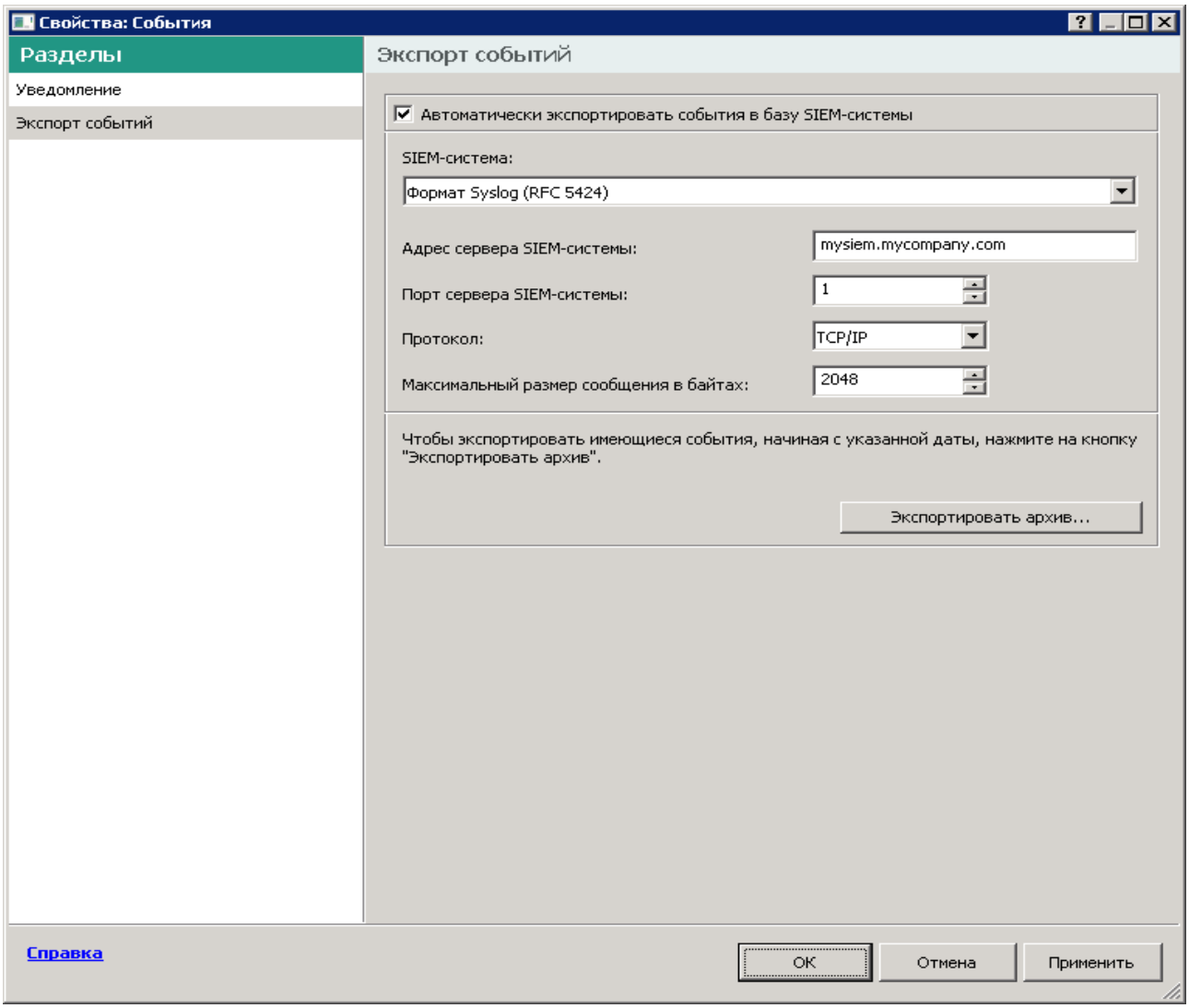


Рисунок 7: Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

  Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

  Выберите вариант **Формат Syslog (RFC 5424)** для передачи событий по протоколу Syslog.

- **Адрес сервера SIEM-системы**

  Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса.

- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

  Выберите протокол передачи сообщений в SIEM-систему. Можно выбрать протокол TCP/IP или UDP. Протокол TCP/IP является более надежным и поддерживает уведомление о получении сообщений. Протокол UDP является более простым, он применяется в случаях, когда проверка и исправление ошибок передачи сообщений не обязательны или выполняются внутри приложения.

- **Максимальный размер сообщения в байтах**

  Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Данное поле доступно только в случае, если вы выбрали формат Syslog в поле **SIEM-система**.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.
6. Нажмите на кнопку **ОК**.

Автоматический экспорт событий включен. После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться в SIEM-систему. Эта процедура описана в разделе "Выбор экспортируемых событий".

Выбор экспортируемых событий

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий во внешнюю систему по одному из следующих условий:

- *Выбор событий в политике*. Если вы выбираете экспортируемые события в политике, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.
- *Выбор событий для отдельной программы*. Если вы выбираете экспортируемые события для отдельной программы, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

В следующих разделах описано, как выбрать экспортируемые события в политике (см. раздел "Выбор событий в политике" на стр. 749) и для отдельной программы (см. раздел "Выбор событий для программы"

на стр. 751).

Выбор событий в политике

Если вы хотите выполнить экспорт событий, произошедших во всех программах, управляемых определенной политикой, выберите экспортируемые события в политике. В этом случае выбор событий для отдельной программы невозможен.

► *Чтобы выбрать экспортируемые события в политике, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.

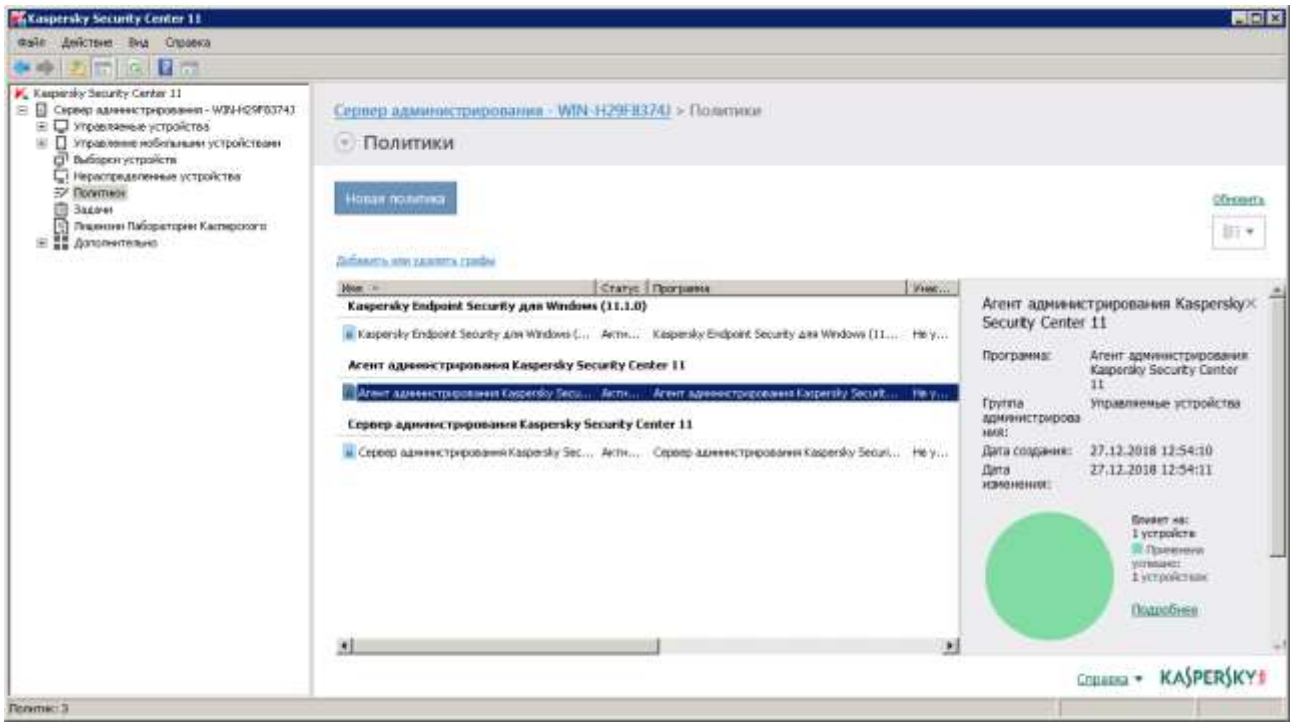
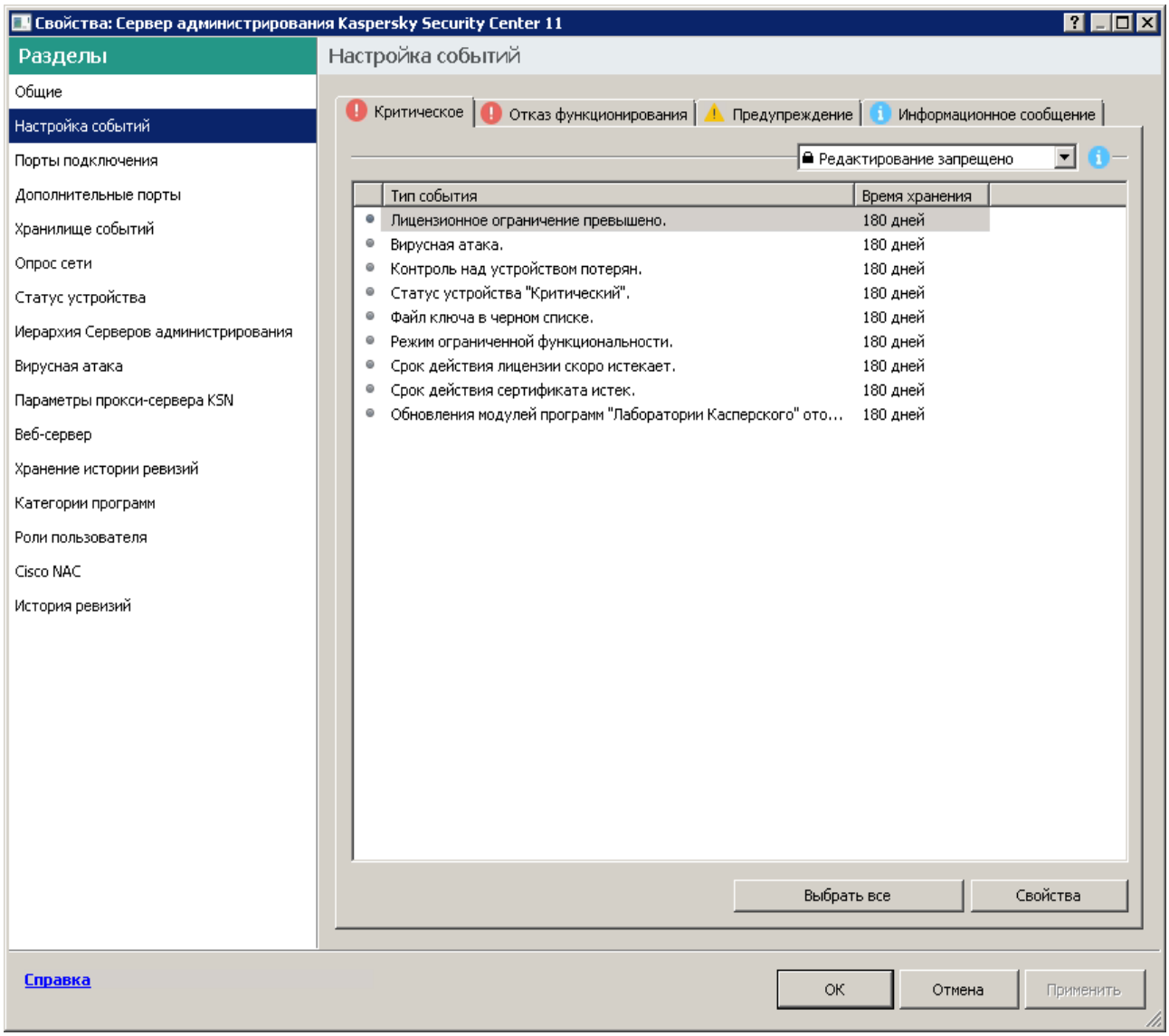


Рисунок 8: Узел Политики

2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.

3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.



4. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

   Если требуется выбрать все события, нажмите на кнопку **Выбрать все**.

5. В появившемся окне свойств событий установите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы включить экспорт для выбранных событий.

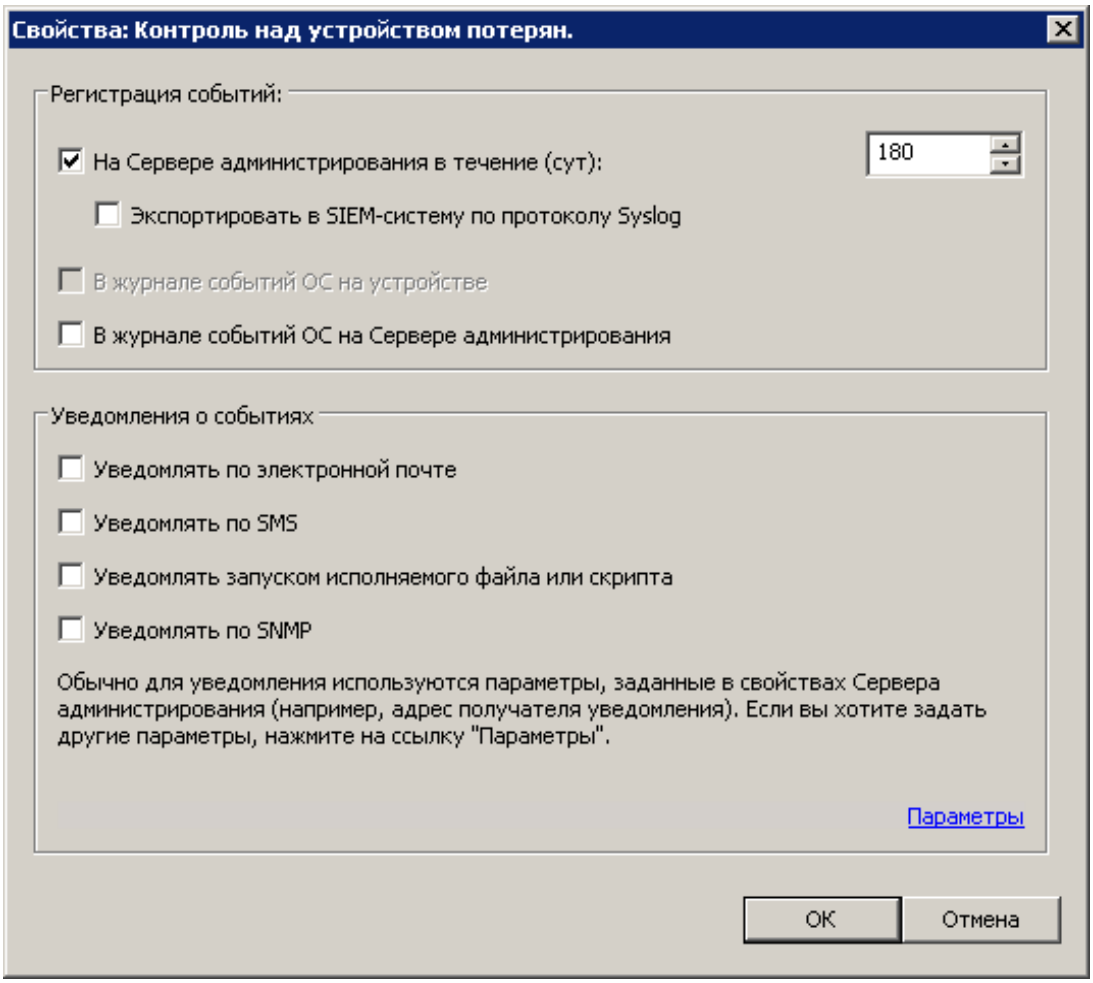


Рисунок 9: Включение экспорта для выбранных событий

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
7. В окне свойств политики нажмите на кнопку **ОК**.

Выбранные события будут отправляться в SIEM-систему по протоколу Syslog. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

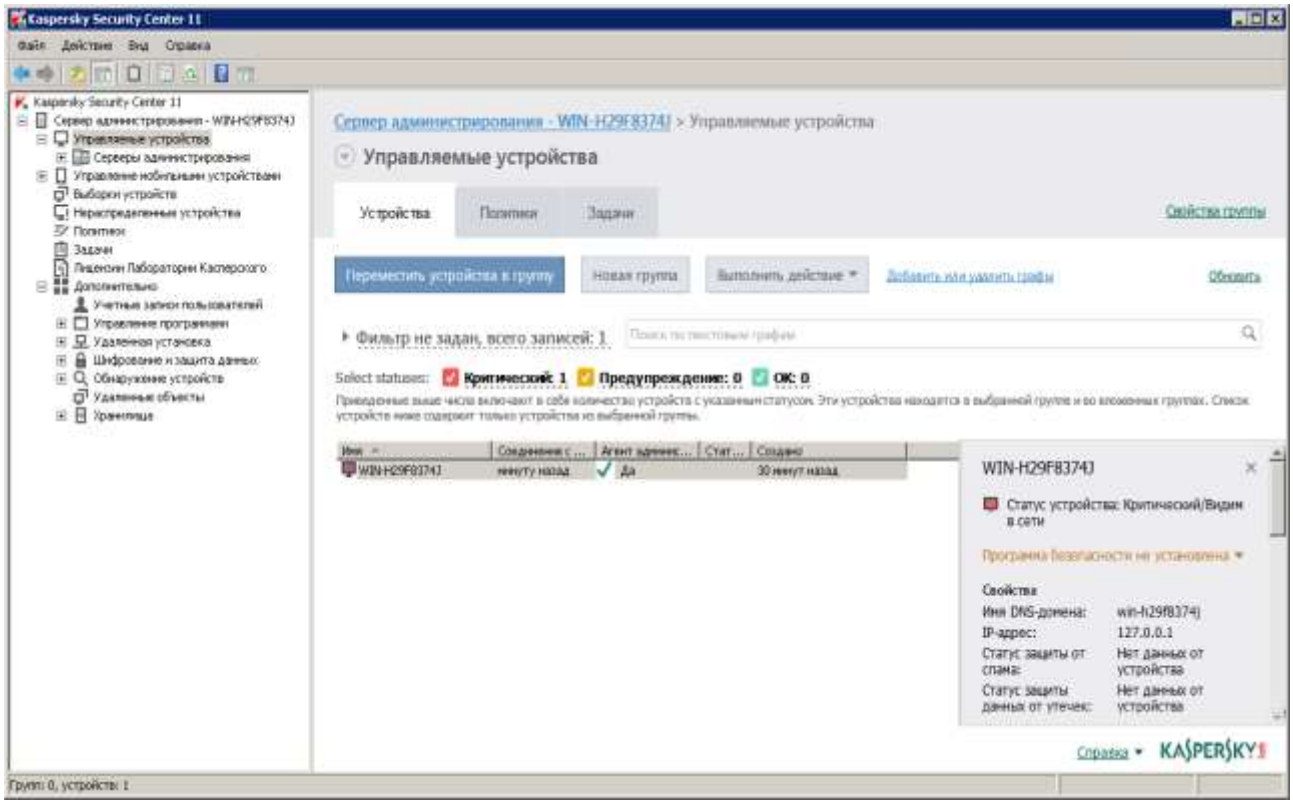
Выбор событий для программы

Если вы хотите выполнить экспорт событий, произошедших в отдельной программе, выберите экспортируемые события для программы. В случае, если ранее экспортируемые события были выбраны в политике, вам не удастся переопределить выбранные события для отдельной программы, управляемой этой политикой.

► *Чтобы выбрать экспортируемые события для отдельной программы, выполните следующие*

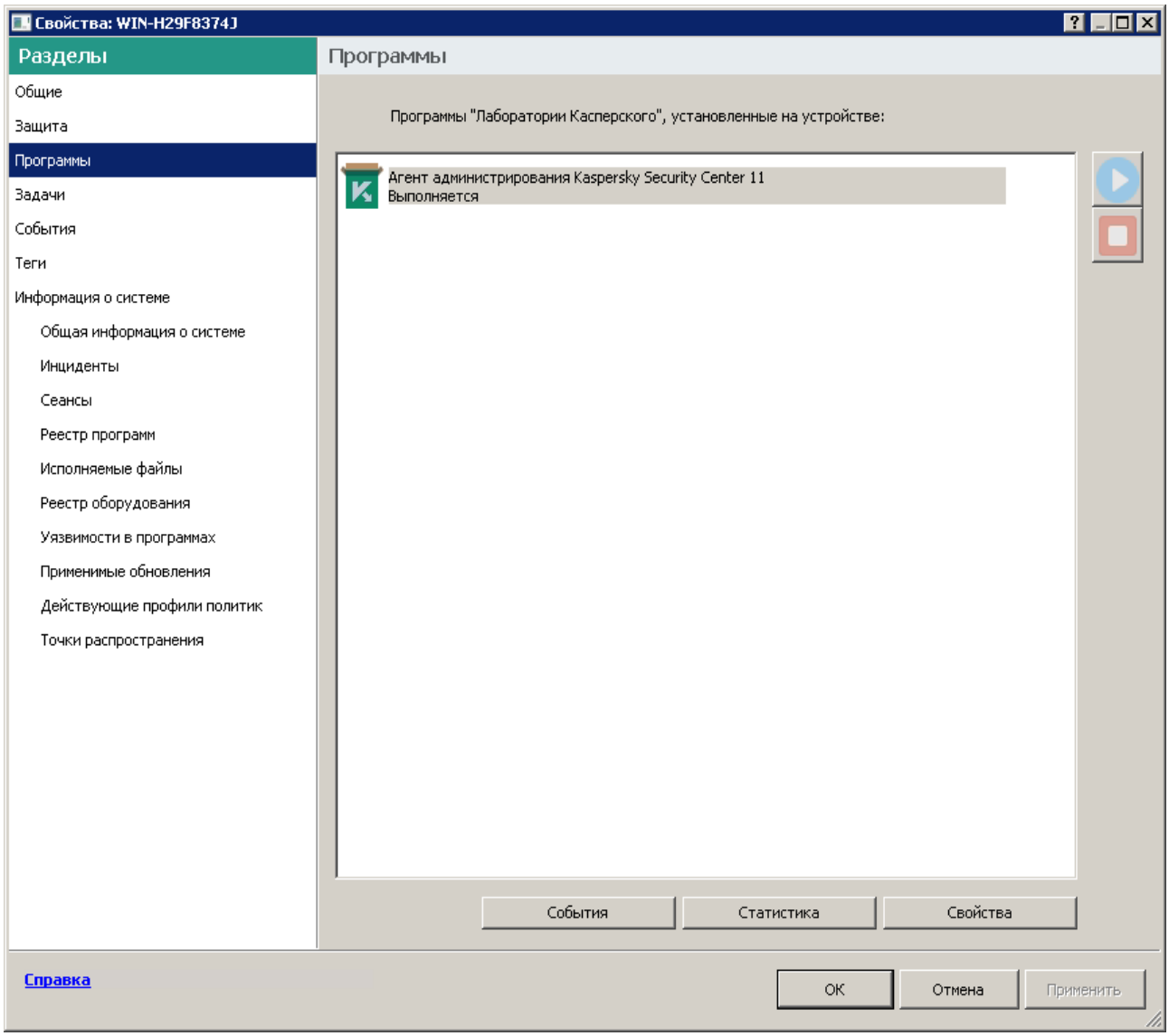
действия:

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на закладку **Устройства**.



2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Программы**.

4. В появившемся списке программ выберите программу, события которой требуется экспортировать, и нажмите на кнопку **Свойства**.



5. В окне свойств программы выберите раздел **Настройка событий**.

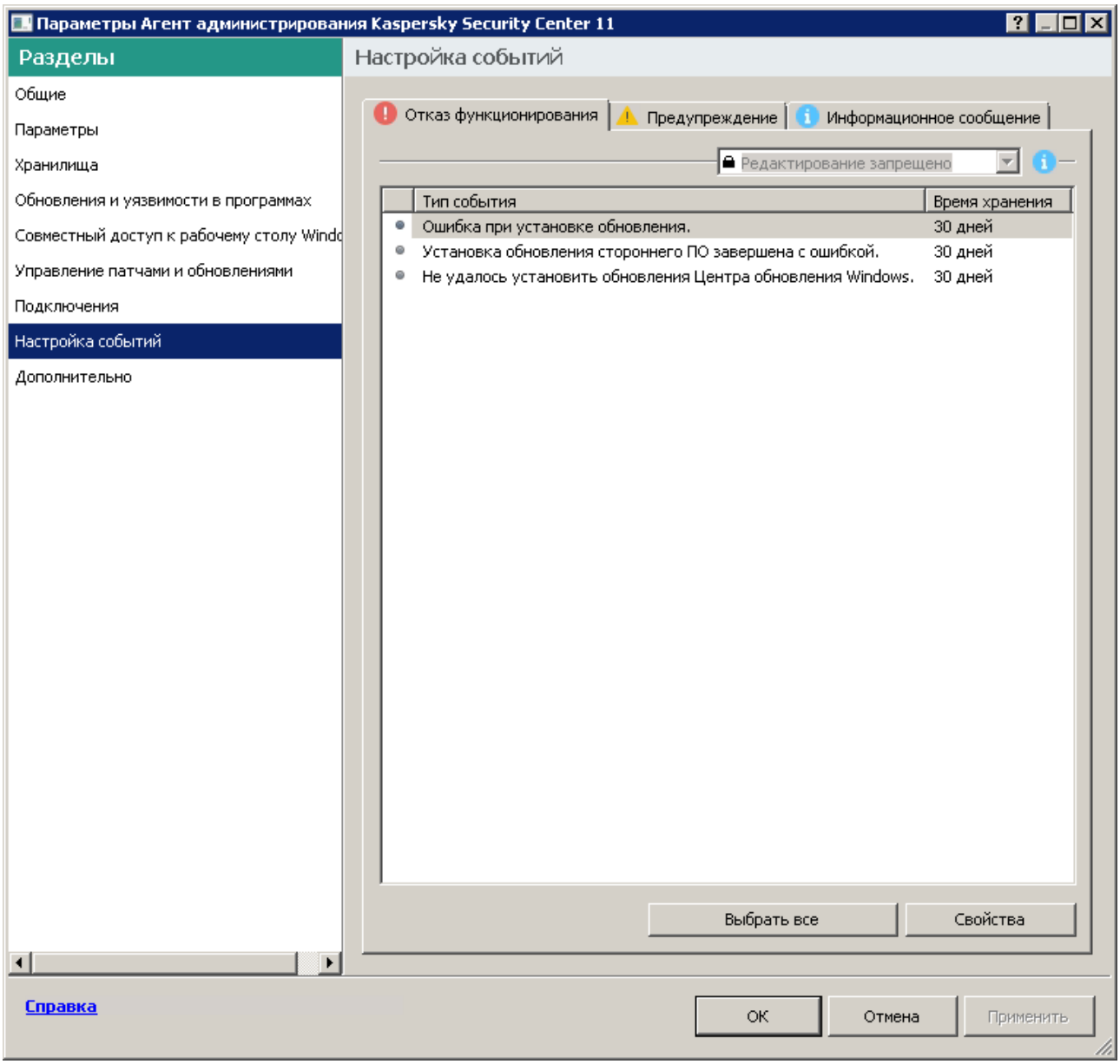


Рисунок 10: Раздел События в окне свойств программы

6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.
7. В появившемся окне свойств событий установите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы включить экспорт для выбранных событий.

Если свойства события заданы в политике, поля этого окна недоступны для редактирования.

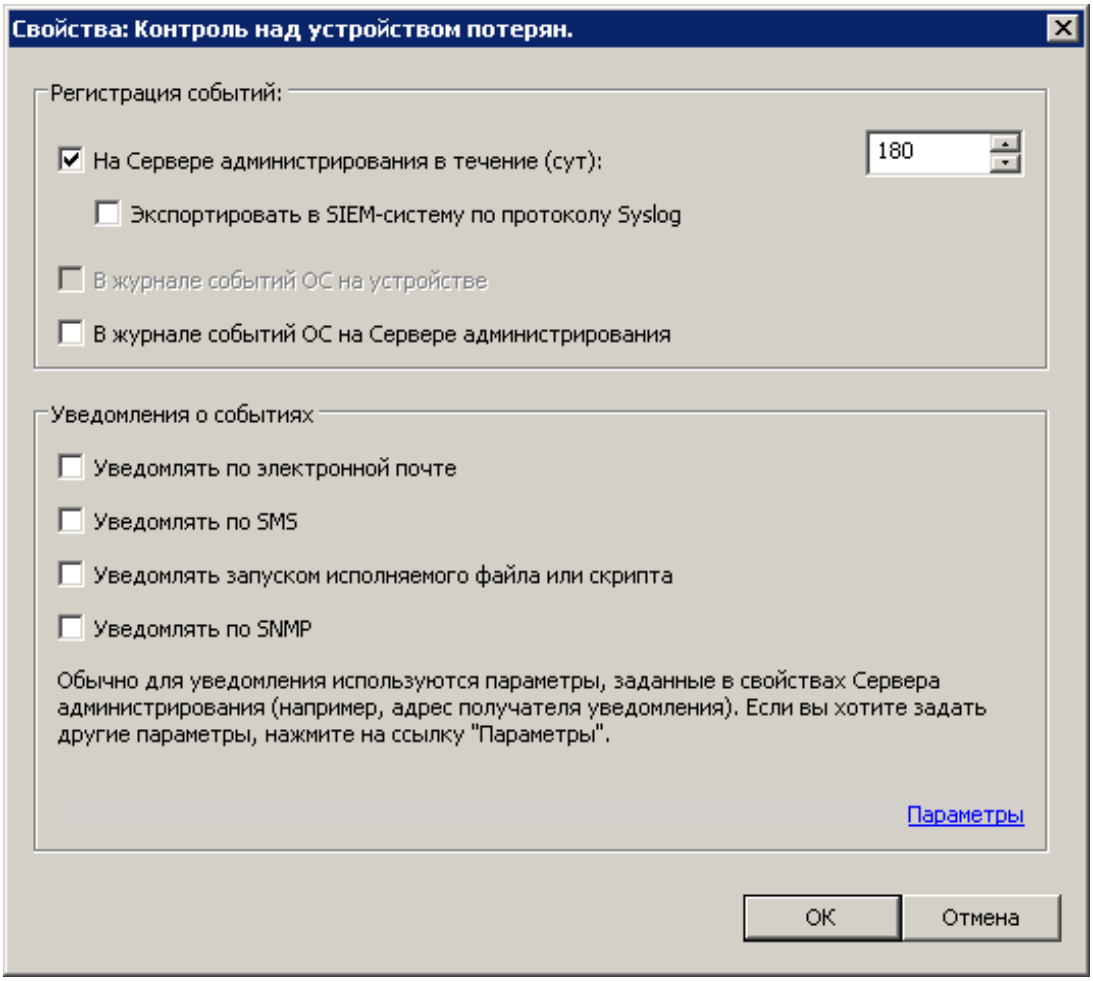


Рисунок 11: Окно свойств событий

8. Нажмите на кнопку **OK**, чтобы сохранить изменения.
9. Нажмите на кнопку **OK** в окне свойств программы и в окне свойств устройства.

Выбранные события будут отправляться в SIEM-систему по протоколу Syslog. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

Экспорт событий по протоколам CEF и LEEF

Протоколы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (см. раздел "Типы событий" на стр. 495) – событий, произошедших на Сервере администрирования или в Агенте администрирования Kaspersky Security Center, а также событий, переданных программами "Лаборатории Касперского" на Сервер администрирования. Набор экспортируемых событий определен заранее,

возможность выбирать экспортируемые события отсутствует.

Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного ключа (см. раздел "Программы "Лаборатории Касперского": лицензирование и активация" на стр. 295).

Протокол экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им протоколы экспорта.

Таблица 64. Протоколы экспорта событий в SIEM-систему

SIEM-система	Протокол экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF – это специализированный формат событий для IBM® Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_logsource_protocols.html).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

В этом разделе

См. также:

Предварительные условия

При настройке автоматического экспорта событий в Консоли администрирования Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

Включение автоматического экспорта общих событий

В Kaspersky Security Center можно включить автоматический экспорт общих событий по протоколу LEEF или CEF.

Только общие события могут быть экспортированы от управляемых программ по протоколам CEF и LEEF. Специфические события программ не могут быть экспортированы от управляемых программ по протоколам CEF и LEEF. Если необходимо экспортировать события управляемых программ или пользовательский набор событий, который настроен с помощью политик управляемых программ, используйте экспорт событий по протоколу Syslog.

► *Чтобы включить автоматический экспорт событий по протоколу CEF или LEEF, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.

3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

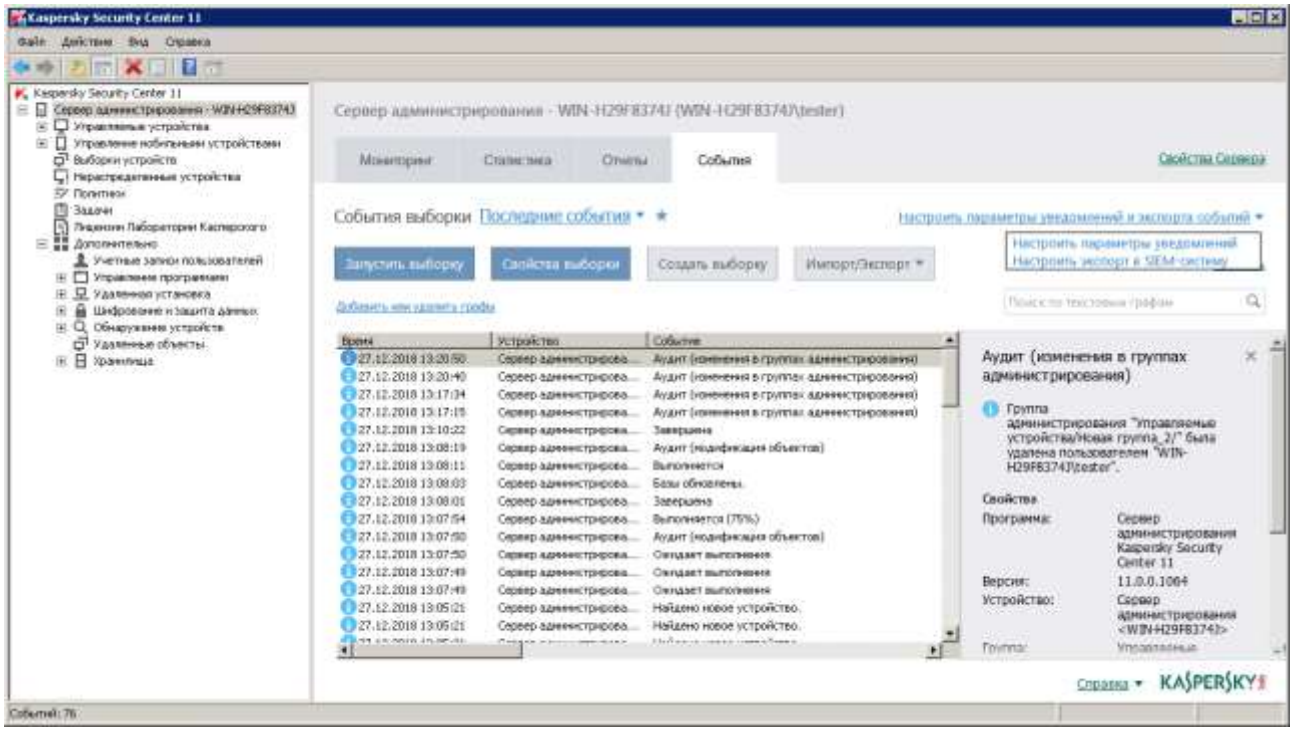


Рисунок 12: Окно свойств событий

Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры:

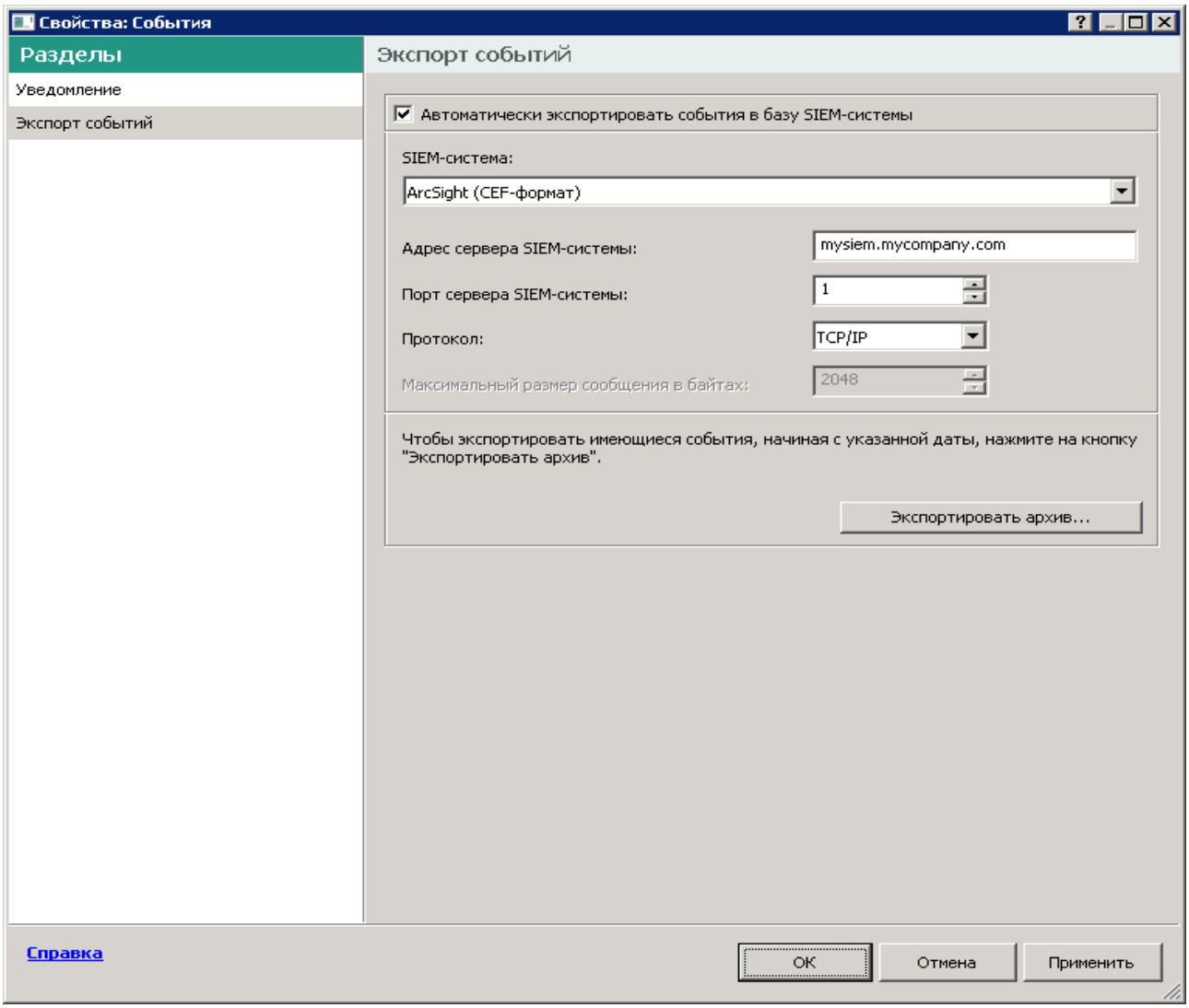


Рисунок 13: Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

  Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

  Выберите, в какую SIEM-систему будет выполняться экспорт событий: QRadar, Splunk или ArcSight.

- **Адрес сервера SIEM-системы**

  Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса.

- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

  Выберите протокол передачи сообщений в SIEM-систему. Можно выбрать протокол TCP/IP или UDP. Протокол TCP/IP является более надежным и поддерживает уведомление о получении сообщений. Протокол UDP является более простым, он применяется в случаях, когда проверка и исправление ошибок передачи сообщений не обязательны или выполняются внутри приложения.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.
6. Нажмите на кнопку **ОК**.

Автоматический экспорт событий будет включен. Общие события будут автоматически экспортироваться в SIEM-систему.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, программам, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие программы для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в

соответствующем разделе (см. раздел "Просмотр имени базы данных Kaspersky Security Center" на стр. 762).

В этом разделе

Создание SQL-запроса с помощью утилиты klsql2

В этом разделе приведены инструкции по загрузке и использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты. При создании SQL-запроса с помощью утилиты klsql2 нет необходимости в явном виде указывать имя и параметры доступа для базы данных Kaspersky Security Center, поскольку запрос обращается напрямую к публичным представлениям Kaspersky Security Center.

► *Чтобы загрузить и использовать утилиту klsql2, выполните следующие действия:*

1. Загрузите утилиту klsql2 (http://media.kaspersky.com/utilities/CorporateUtilities/klsql2.zip) с веб-сайта "Лаборатории Касперского".
2. Скопируйте и извлеките содержимое архива klsql2.zip в любую папку на устройстве, на котором установлен Сервер администрирования Kaspersky Security Center.

   Пакет klsql2.zip содержит следующие файлы:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Откройте файл src.sql с помощью любого текстового редактора.
4. Выполните следующие действия с файлом src.sql:
   a. Удалите содержимое файла src.sql.
   b. В файле src.sql введите требуемый SQL-запрос.
   c. Сохраните файл src.sql.
5. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Откройте созданный файл result.xml и посмотрите результаты выполнения запроса.

Вы можете редактировать файл src.sql и создавать в нем любые запросы к публичным представлениям.

Затем с помощью команды в командной строке можно запустить запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

Пример:

```
SELECT
e.nId,                                  /* идентификатор события */
e.tmRiseTime,                                /* время возникновения события */
e.strEventType,                              /* внутреннее имя типа события */
e.wstrEventTypeDisplayName,                  /* отображаемое имя события */
e.wstrDescription,                           /* отображаемое описание события */
e.wstrGroupName,                        /* имя группы устройств */
h.wstrDisplayName,                           /* отображаемое имя устройства, на
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp      /* IP-адрес устройства, на ко
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Просмотр имени базы данных Kaspersky Security Center

Для доступа к базе данных Kaspersky Security Center с помощью SQL Server или MySQL необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

► *Чтобы просмотреть имя базы данных Kaspersky Security Center, выполните следующие действия:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В появившемся окне свойств Сервера администрирования выберите пункт **Дополнительно**, а затем **Информация об используемой базе данных**.
3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных:
   - **Имя экземпляра**

Имя экземпляра используемой базы данных Kaspersky Security Center. Значение по умолчанию – *.\KAV_CS_ADMIN_KIT.*

- **Имя базы данных**

  Имя базы данных SQL Kaspersky Security Center. По умолчанию указано значение *KAV*.

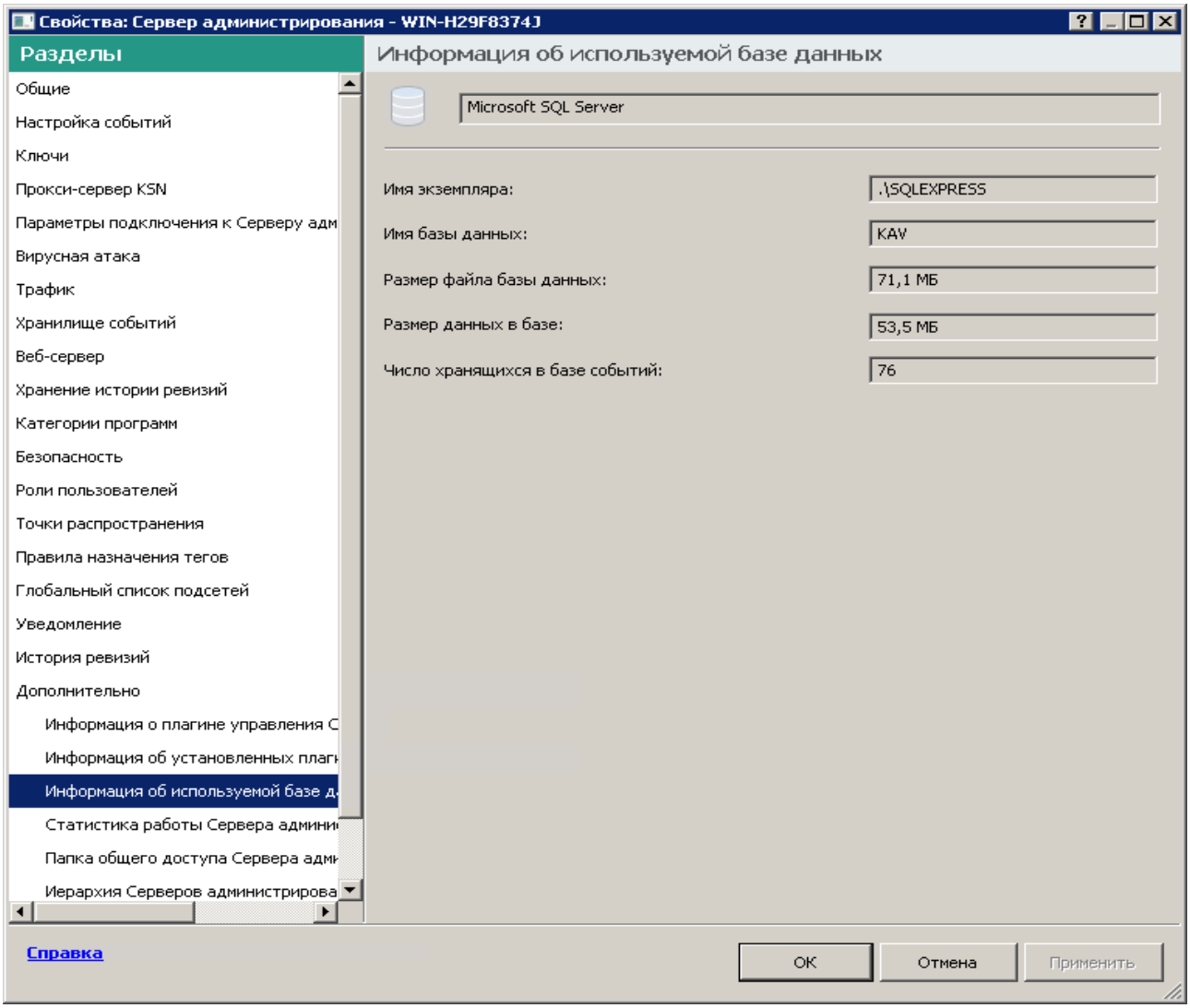


Рисунок 14: Имя базы данных SQL Kaspersky Security Center

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

Настройка экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center – и получатель событий – SIEM-система. Экспорт

событий необходимо настроить в используемой SIEM-системе и в Консоли администрирования Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

  Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

  Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

  Протокол, используемый для экспорта событий в SIEM-систему. Это может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На следующем рисунке приведен пример настройки приемника в ArcSight.

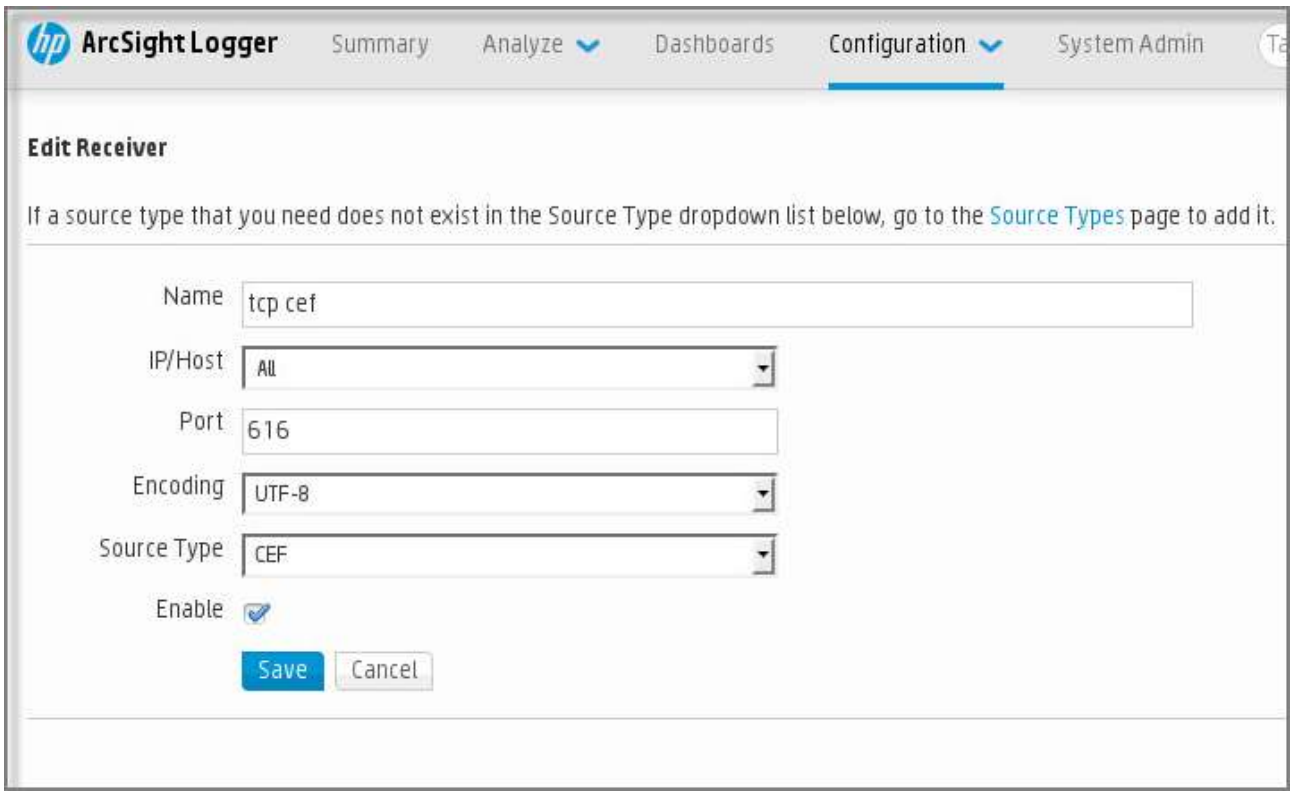


Рисунок 15: Пример настройки приемника сообщений

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

В каждой SIEM-системе имеется набор стандартных анализаторов сообщений. "Лаборатория Касперского" также предоставляет анализаторы сообщений для некоторых SIEM-систем, например, для QRadar и ArcSight. Вы можете загрузить эти анализаторы сообщений с веб-страниц соответствующих SIEM-систем. При настройке приемника можно выбрать используемый анализатор сообщений: один из стандартных анализаторов вашей SIEM-системы или анализатор, предоставляемый "Лабораторией Касперского".

Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте

и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. На рисунке видно, что первое событие относится к критическим событиям Сервера администрирования – *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

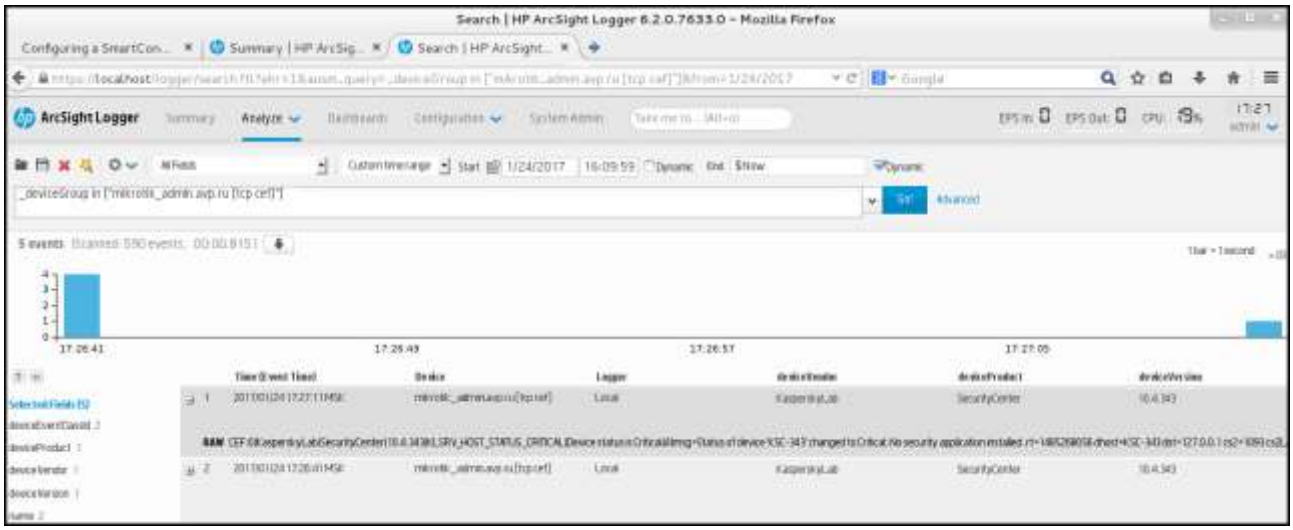


Рисунок 16: Пример событий

Работа в облачном окружении

В этом разделе представлена информация о развертывании и обслуживании Kaspersky Security Center в облачных окружениях, таких как Amazon Web Services и Microsoft Azure.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

В этом разделе

О работе в облачном окружении

Kaspersky Security Center 11 работает не только с физическими устройствами, но также предоставляет возможность для работы в облачном окружении. Kaspersky Security Center работает с инстансами Amazon EC2 (далее также *инстансы*) и с виртуальными машинами Microsoft Azure. Инстанс Amazon EC2 это виртуальная машина, которая создана на основе платформы Amazon Web Services (AWS).

Для работы с инстансами Amazon EC2 Kaspersky Security Center использует AWS *API* (AWS Application Program Interface, программный интерфейс приложения AWS). Чтобы работать с виртуальными машинами

Azure, программа Kaspersky Security Center должна использовать Azure API.

Вы можете развернуть Kaspersky Security Center на инстансе Amazon EC2 или на виртуальной машине Microsoft Azure для управления защитой устройств в облачном окружении и пользоваться специальными возможностями Kaspersky Security Center для работы в облачном окружении. Эти возможности включают:

- опрос инстансов, находящихся в облачном окружении, средствами AWS API;
- использование инструментов API для установки Агента администрирования и программ безопасности на устройствах в облачном окружении;
- поиск виртуальных машин по признаку принадлежности к определенному облачному сегменту.

Вы также можете использовать инстанс или виртуальную машину, на которых развернут Сервер администрирования Kaspersky Security Center, для защиты физических устройств (например, если такой облачный сервер оказывается выгоднее в обслуживании и содержании, чем физический). В этом случае работа с Сервером администрирования будет устроена так же, как если бы Сервер администрирования был установлен на физическом устройстве.

В Kaspersky Security Center, развернутом с платного Amazon Machine Image (AMI) (в AWS) или используемом на основе подписки с ежемесячной тарификацией в зависимости от объема услуг (в Azure), возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

Сервер администрирования устанавливается совместно с Консолью администрирования. Kaspersky Security для Windows Server также автоматически устанавливается на устройство, на котором установлен Сервер администрирования.

Используйте мастер настройки для работы в облачном окружении (см. стр. 800), чтобы настроить Kaspersky Security Center с учетом особенностей работы в облачном окружении.

Сценарий: Развертывание в облачном окружении

В этом разделе описан сценарий развертывания Kaspersky Security Center для работы в облачном окружении, таком как Amazon Web Services и Microsoft Azure.

После завершения сценария развертывания будут запущены и настроены с параметрами по умолчанию Сервер администрирования Kaspersky Security Center (см. раздел "Сервер администрирования" на стр. 33) и Консоль администрирования. На выбранных инстансах Amazon EC2 / виртуальных машинах Microsoft Azure будет развернута антивирусная защита под управлением Kaspersky Security Center. В дальнейшем вы можете настраивать Kaspersky Security Center более подробно, создавать сложную структуру групп администрирования, создавать для групп различные политики и задачи.

Требования

1. Подготовка.
2. Развертывание Сервера администрирования.
3. Установка антивирусных программ "Лаборатории Касперского" на виртуальные устройства, которые необходимо защитить.
4. Настройка параметров загрузки обновлений.
5. Настройка параметров работы с отчетами о состоянии защиты устройств.

Для первоначальной настройки существует мастер настройки для работы в облачном окружении (см. стр. 800). Он запускается автоматически при первом запуске Kaspersky Security Center, развернутого из готового образа. Вы также можете запустить мастер вручную в любой момент. Кроме того, вы можете самостоятельно выполнить все действия, которые выполняет мастер.

Рекомендуется отвести на развертывание Сервера администрирования Kaspersky Security Center в облачном окружении не менее часа, а всего на развертывание защиты в облачном окружении – не менее одного рабочего дня.

Развертывание Kaspersky Security Center в облачном окружении Amazon Web Services состоит из следующих этапов:

a. **Планирование конфигурации облачных сегментов**

   Ознакомьтесь с работой Kaspersky Security Center в облачном окружении (см. раздел "О работе в облачном окружении Amazon Web Services" на стр. 776). Планирование, где будет развернут Сервера администрирования: на инстансе Amazon EC2 / виртуальных машинах Microsoft Azure либо вне облачного окружения; определите также, сколько облачных сегментов вы планируете защищать. Если вы планируете разместить Сервер администрирования вне облачного окружения, либо если вы планируете защищать более 5000 устройств, то вам потребуется установить Сервер администрирования самостоятельно.

b. **Планирование ресурсов**

   Убедитесь, что выполнены все условия, необходимые для развертывания (см. раздел "Предварительные условия для развертывания Kaspersky Security Center в облачном окружении" на стр. 773).

c. **Подписка на Kaspersky Security Center в виде готового образа в магазине Marketplace**

   Выберите один из готовых образов AMI в магазине AWS Marketplace или выберите использование ежемесячных счетов за использование SKU в магазине Azure Marketplace, оплатите в соответствии с правилами магазина, если необходимо (или используйте модель BYOL), и используйте образ для развертывания инстанса Amazon EC2 / виртуальной машины Microsoft Azure с установленной программой Kaspersky Security Center.

   Этот шаг необходим, только если вы планируете разместить Сервер администрирования на инстансе / виртуальной машине внутри облачного окружения и при этом планируете разворачивать защиту не более чем 5000 устройств. Иначе этот этап не нужен, и вместо него вам нужно самостоятельно установить Сервер администрирования, Консоль администрирования и СУБД (см. раздел "Основной сценарий развертывания и другие сценарии развертывания" на стр. 49).

d. Определение местоположения СУБД

Определение, где будет расположена СУБД (см. раздел "Параметры базы данных для работы в облачном окружении" на стр. 774). Если вы хотите использовать СУБД Amazon RDS или Microsoft Azure SQL, создайте базу данных с Relational Database Service (RDS) в облачном окружении AWS или со службой базы данных Azure в облачном окружении Microsoft Azure (см. раздел "Работа с Azure SQL" на стр. 794). Если вы хотите использовать базу данных вне облачного окружения, убедитесь, что у вас есть рабочая база данных.

e. Установка Сервера администрирования и Консоли администрирования (на основе Microsoft Management Console и / или на основе веб-приложения) на выбранных устройствах вручную

Установите Сервер администрирования, Консоль администрирования и СУБД на выбранные устройства так, как предусматривает основной сценарий развертывания Kaspersky Security Center (см. раздел "Основной сценарий развертывания и другие сценарии развертывания" на стр. 49).

Этот этап необходим, если вы планируете разместить Сервер администрирования вне облачного окружения или если вы планируете разворачивать защиту более чем 5000 устройств. Иначе этот этап не нужен и достаточно подписки на Kaspersky Security Center в виде готового образа в магазине AWS Marketplace или Azure Marketplace.

f. Обеспечение прав для работы Сервера администрирования с облачными-службами API

В AWS создайте в Консоли управления AWS либо IAM-роль (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 777) , либо учетную запись IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780). Созданная IAM-роль (либо учетная запись IAM-пользователя) позволит Kaspersky Security Center работать с AWS API: опрашивать облачные сегменты и разворачивать защиту.

В Azure, создайте подписку и ИД приложения с паролем (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791). Kaspersky Security Center использует эти учетные данные для работы в AWS API: для опроса облачных сегментов и развертывания защиты.

g. Создание IAM-роли для защищаемых инстансов (только для AWS)

Создайте в Консоли управления AWS IAM-роль (см. раздел "Создание IAM-роли для установки программ на инстансы Amazon EC2" на стр. 781), которая определяет набор разрешений для выполнения запросов к AWS. Созданную роль вы впоследствии будете назначать новым инстансам. IAM-роль нужна для установки программ на инстансы с помощью Kaspersky Security Center.

h. Подготовка базы данных с помощью Amazon Relational Database Service или Microsoft Azure SQL

Если вы планируете использовать базу данных Amazon Relational Database Service (RDS) (см. раздел "Работа с Amazon RDS" на стр. 782), создайте инстанс базы данных Amazon RDS и корзина S3, где будет храниться резервная копия базы данных. Вы можете пропустить этот этап, если вам нужна база данных на том же экземпляре EC2, где установлен Сервер администрирования, или если вы хотите, чтобы ваша база данных находилась в другом месте (см. раздел "Параметры базы данных для работы в облачном окружении" на стр. 774).

Если вы планируете использовать Microsoft Azure SQL, создайте учетную запись хранилища (см. раздел "Создание учетной записи хранения Azure" на стр. 794) и базу данных в Microsoft Azure (см. раздел "Создание базы данных Azure SQL и SQL-сервера" на стр. 795).

i. **Лицензирование Kaspersky Security Center для работы в облачном окружении**

Убедитесь, что у вас есть лицензия (см. раздел "Варианты лицензирования в облачном окружении" на стр. 773) для работы Kaspersky Security Center в облачном окружении, и предоставьте код активации либо файл ключа, чтобы программа добавила его в хранилище лицензий. Это шаг может быть завершен в мастере настройки для работы в облачном окружении (см. раздел "Шаг 1.Выбор способа активации программы" на стр. 802).

Этот этап обязателен, если вы используете Kaspersky Security Center, установленный из бесплатного готового образа AMI по модели BYOL, или если вы устанавливаете Kaspersky Security Center самостоятельно без использования образов AMI. В каждом из этих случаев для активации Kaspersky Security Center вам нужна лицензия на программу Kaspersky Security для виртуальных сред или на программу Kaspersky Hybrid Cloud Security.

Если вы используете Kaspersky Security Center, установленный из платного готового образа, то этот этап является необязательным и соответствующее окно мастера настройки для работы в облачном окружении не отображается.

j. **Аутентификация в облачном окружении**

Укажите в Kaspersky Security Center ваши учетные данные AWS или Azure, чтобы Kaspersky Security Center мог работать с необходимыми разрешениями. Это шаг может быть завершен в мастере настройки для работы в облачном окружении (см. раздел "Шаг 3. Аутентификация в облачном окружении" на стр. 803).

k. **Получение Сервером администрирования сведений об устройствах в облачном сегменте путем опроса облачного сегмента**

Запустите опрос облачного сегмента (см. раздел "Опрос облачного сегмента" на стр. 813). В облачном окружении AWS Kaspersky Security Center получит адреса и имена всех инстансов, доступ к которым обеспечивают права IAM-роли или права IAM-пользователя. В облачном окружении Microsoft Azure Kaspersky Security Center получит адреса и имена всех виртуальных машин, доступ к которым обеспечивают права роли Читатель.

В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные инстансы / виртуальные машины.

Kaspersky Security Center запускает опрос регулярно, поэтому, если появятся новые инстансы / виртуальные машины, то они будут обнаружены автоматически.

l. **Объединение всех устройств сети в группу администрирования Cloud**

Переместите все обнаруженные инстансы / виртуальные машины в группу администрирования **Управляемые устройства\Cloud**, чтобы они стали доступными для централизованного управления. Если вы хотите разбить устройства на подгруппы, например, в зависимости от того, какая операционная система на них установлена, вы можете создать несколько групп администрирования внутри группы **Управляемые устройства\Cloud**. Вы можете настроить автоматическое перемещение (см. раздел "Создание правил автоматического перемещения устройств в группы администрирования" на стр. 248) всех устройств, которые будут обнаружены во время регулярных опросов, в группу **Управляемые устройства\Cloud**.

m. **Связь устройств в сети с Сервером администрирования с помощью Агента администрирования**

Установите Агента администрирования на устройствах в облачном окружении (см. раздел "Установка программ на устройства в облачном окружении" на стр. 821). (Компонент Kaspersky Security Center обеспечивает связь устройства с Сервером администрирования.) Параметры Агента администрирования автоматически настраиваются по умолчанию.

Вы можете установить Агент администрирования на каждое устройство локально (см. раздел "Установка программ на клиентские устройства" на стр. 672). Вы также можете установить Агент администрирования на устройства удаленно, с помощью Kaspersky Security Center (см. раздел "Создание инсталляционных пакетов программ" на стр. 670). Или вы можете пропустить этот этап и установить Агент администрирования вместе с последними версиями программ безопасности.

n. **Установка последних версий программ безопасности на устройства сети**

Выберите устройства, на которые вы хотите установить программы безопасности, и установите на эти устройства последние версии программ безопасности (см. раздел "Установка программ на клиентские устройства" на стр. 672). Вы можете произвести установку либо удаленно, с помощью Kaspersky Security Center на Сервере администрирования, либо локально.

Для инстансов и виртуальных машин под управлением Linux предназначена программа Kaspersky Endpoint Security для Linux.

Для инстансов и виртуальных машин под управлением Windows предназначена программа Kaspersky Security для Windows Server.

o. **Настройка параметров обновлений**

Задача **Поиск уязвимостей и требуемых обновлений** создается автоматически во время работы мастера настройки для работы в облачном окружении. Вы также можете создать ее вручную (см. раздел "Поиск уязвимостей в программах" на стр. 403). Эта задача обеспечивает автоматический поиск и загрузку необходимых обновлений программ для последующей установки на устройства в сети средствами Kaspersky Security Center.

Следующие этапы рекомендуется выполнять после завершения работы мастера настройки для работы в облачном окружении:

p. **Настройка работы с отчетами**

Вы можете просматривать отчеты (см. раздел "Работа с отчетами" на стр. 462) на закладке **Мониторинг** в рабочей области узла **Сервер администрирования** и / или получать отчеты по электронной почте. Отчеты на закладке **Мониторинг** доступны по умолчанию. Чтобы настроить получение отчетов по электронной почте, укажите адреса электронной почты, на которые будут приходить отчеты, и настройте формат отчетов.

Результаты

После завершения сценария, убедитесь (см. раздел "Проверка успешности настройки" на стр. 812), что провели первоначальную настройку успешно:

- Вы можете подключится к Серверу администрирования с помощью Консоли администрирования.
- На управляемых устройствах установлены и работают последние версии программ безопасности

"Лаборатории Касперского".

- Kaspersky Security Center создал для всех управляемых устройств политики и задачи по умолчанию.

Предварительные условия для развертывания Kaspersky Security Center в облачном окружении

Перед началом развертывания Kaspersky Security Center в облачном окружении, таком как Amazon Web Services или Microsoft Azure, убедитесь, что у вас имеется:

- доступ в интернет;
- учетная запись Amazon Web Services или Microsoft;
- одно из следующих:
  - лицензия на Kaspersky Security для виртуальных сред;
  - лицензия на Kaspersky Hybrid Cloud Security;
  - средства на приобретение такой лицензии;
  - средства на оплату в магазине Azure Marketplace готового образа;
- руководства к последним версиям программ Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server.

Варианты лицензирования в облачном окружении

Работа в облачном окружении не входит в базовую функциональность Kaspersky Security Center и требует лицензии.

В Kaspersky Security Center доступно два варианта лицензирования для работы в облачном окружении:

- Платный образ AMI (в Amazon Web Services) / Использование ежемесячных счетов за использование SKU (в Microsoft Azure).

  Такой вариант лицензирования Kaspersky Security Center предоставляет также лицензию для Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server. Вы должны оплатить лицензию согласно правилам Amazon Marketplace или Azure Marketplace.

  Эта модель позволяет вам управлять не более чем 200 клиентскими устройствами для одного Сервера администрирования.

- Готовый бесплатный образ с использованием собственной лицензии по модели BYOL (Bring Your Own License).

  Для лицензирования Kaspersky Security Center в AWS или Azure необходима лицензия на использование одной из программ:

  - Kaspersky Security для виртуальных сред;

- Kaspersky Hybrid Cloud Security.

Эта модель позволяет вам управлять до 100 000 клиентских устройств для одного Сервера администрирования. Эта модель также позволяет вам управлять устройствами вне облачного окружения AWS (или Azure).

Вы можете выбрать модель BYOL в следующих случаях:

- у вас уже есть действующая лицензия на Kaspersky Security виртуальных сред;
- у вас уже есть действующая лицензия на Kaspersky Hybrid Cloud Security;
- вы хотите приобрести лицензию непосредственно перед развертыванием Kaspersky Security Center.

На этапе первоначальной настройки (см. раздел "Шаг 1.Выбор способа активации программы" на стр. 802), Kaspersky Security Center запрашивает у вас код активации или файл ключа.

При выборе BYOL вам не нужно будет оплачивать использование Kaspersky Security Center через магазин Azure Marketplace или AWS Marketplace.

В обоих случаях возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

После подписки на Kaspersky Security Center вы получаете Amazon Elastic Compute Cloud (Amazon EC2) или виртуальную машину Microsoft Azure с Сервером администрирования Kaspersky Security Center. Инсталляционные пакеты Kaspersky Security для Windows Server и Kaspersky Endpoint Security для Linux доступны на Сервере администрирования. Вы можете установить эти программы на устройствах в облачном окружении. Вам не нужно активировать эти программы по лицензии.

Если управляемое устройство не видимо в сети Сервера администрирования более недели, программа безопасности (Kaspersky Security для Windows Server или Kaspersky Endpoint Security для Linux) на этом устройстве перейдет в режим ограниченной функциональности. Чтобы активировать программу снова, вы должны сделать устройство, на котором установлена программа безопасности, видимым в сети Сервера администрирования снова.

Параметры базы данных для работы в облачном окружении

У вас должна быть база данных для работы с Kaspersky Security Center. При развертывании Kaspersky Security Center в AWS или в Microsoft Azure у вас есть три параметра:

- Создайте локальную базу данных на одном устройстве с Сервером администрирования. Kaspersky Security Center поставляется вместе с базой данных SQL Server Express, которая может поддерживать до 5000 управляемых устройств. выберите этот параметр, если базы данных SQL Server Express Edition достаточно для ваших потребностей.

- Создайте базу данных с Relational Database Service (RDS) в облачном окружении AWS или со службой базы данных Azure в облачном окружении Microsoft Azure (см. раздел "Работа с Azure SQL" на стр. 794). Выберите этот параметр, если вы хотите использовать СУБД, отличную от SQL Express. Ваши данные будут перенесены в облачное окружение, где они останутся, и у вас не будет никаких дополнительных затрат. Если вы уже работаете с Kaspersky Security Center локально и имеете некоторые данные в своей базе данных, вы можете перенести свои данные в новую базу данных.
- Используйте существующий сервер базы данных. Выберите этот параметр, если вы уже используете сервер базы данных и хотите использовать его для Kaspersky Security Center. Если этот сервер расположен все облачного окружения, ваши данные будут перенесены через интернет, что может привести к дополнительным расходам.

Процедура развертывания Kaspersky Security Center в облачном окружении имеет специфические шаги для создания (выбора) базы данных.

Работа в облачном окружении Amazon Web Services

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center в Amazon Web Services.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

В этом разделе

О работе в облачном окружении Amazon Web Services

Вы можете приобрести Kaspersky Security Center в магазине приложений AWS Marketplace в виде образа AMI (Amazon Machine Image) – готового образа предварительно настроенной виртуальной машины. Вы можете подписаться на платный готовый образ AMI или BYOL AMI и на основе этого образа создать инстанс Amazon EC2 с установленным Kaspersky Security Center.

Для работы с платформой AWS, и в частности для того, чтобы приобретать приложения в AWS Marketplace и создавать инстансы, вам потребуется учетная запись в Amazon Web Services. Вы можете создать бесплатную учетную запись на сайте https://aws.amazon.com. Вы также можете использовать существующую учетную запись Amazon.

Если вы подписались на AMI, доступный в магазине приложений AWS Marketplace, то вы получаете инстанс с готовым к работе Kaspersky Security Center. Вам не нужно устанавливать программу самостоятельно. Kaspersky Security Center в этом случае устанавливается на инстанс без вашего участия. После установки вы можете запустить Консоль администрирования и подключиться к Серверу администрирования, чтобы начать работу с Kaspersky Security Center.

О том, что такое образы AMI и как работает магазин приложений AWS Marketplace, см. на странице справки AWS Marketplace (https://aws.amazon.com/marketplace/help). О работе с платформой AWS, об использовании инстансов и о связанных с ними понятиях см. в документации Amazon Web Services https://aws.amazon.com/documentation/.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Создание IAM-роли и учетных записей IAM-пользователя для инстансов Amazon EC2

В этом разделе описано, какие действия необходимо выполнить, чтобы обеспечить корректную работу Сервера администрирования. Эти действия включают работу с сервисами AWS, с IAM-ролями (Access Management) и учетными записями пользователей. Также описано, какие действия должны быть выполнены с клиентскими устройствами, чтобы установить на них Агент администрирования и затем защитные программы Kaspersky Security для Windows Server и Kaspersky Endpoint Security для Linux.

Вы можете подготовить инстанс EC2 вручную или автоматически, с использованием скрипта.

В этом разделе

Обеспечение прав для работы Сервера администрирования Kaspersky Security Center с AWS

Стандарты работы в облачной среде Amazon Web Services рекомендуют (см. раздел http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html), чтобы специальная IAM-роль (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 777) была назначена экземпляру Сервера администрирования для работы со службами AWS. Создайте в консоли AWS IAM-роль, которая определяет набор разрешений для выполнения запросов к сервисам AWS. IAM-роль обеспечивает права на опрос облачных сегментов и на установку программ на инстансы.

После того как вы создадите IAM-роль и назначите ее на Сервер администрирования, вы сможете разворачивать защиту инстансов, пользуясь этой ролью и не предоставляя Kaspersky Security Center никакой дополнительной информации.

Однако в следующих случаях может быть целесообразно отказаться от создания IAM-роли для Сервера администрирования:

- Если устройства, защитой которых вы планируете управлять, являются инстансами EC2 внутри облачного окружения Amazon Web Services, а Сервер администрирования находится вне него.
- Если вы планируете управлять защитой инстансов не только внутри вашего облачного сегмента, но и внутри других облачных сегментов, созданных под другой учетной записью в AWS. В таком случае вам понадобится IAM-роль только для защиты вашего облачного сегмента. Для защиты другого облачного сегмента IAM-роль не понадобится.

IB этих случаях вам потребуется создать не IAM-роль, а *учетную запись IAM-пользовател* (см. раздел "*Создание учетной записи IAM-пользователя для работы Kaspersky Security Center*" на стр. 780), от имени которого Kaspersky Security Center будет работать с сервисами AWS. Прежде чем начинать работу с Сервером администрирования, создайте учетную запись IAM-пользователя с *ключом доступа AWS IAM* (далее также *ключ доступа IAM*).

Для создания IAM-роли либо IAM-пользователя требуется Консоль управления AWS https://console.aws.amazon.com. Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

Создание IAM-роли для Сервера администрирования

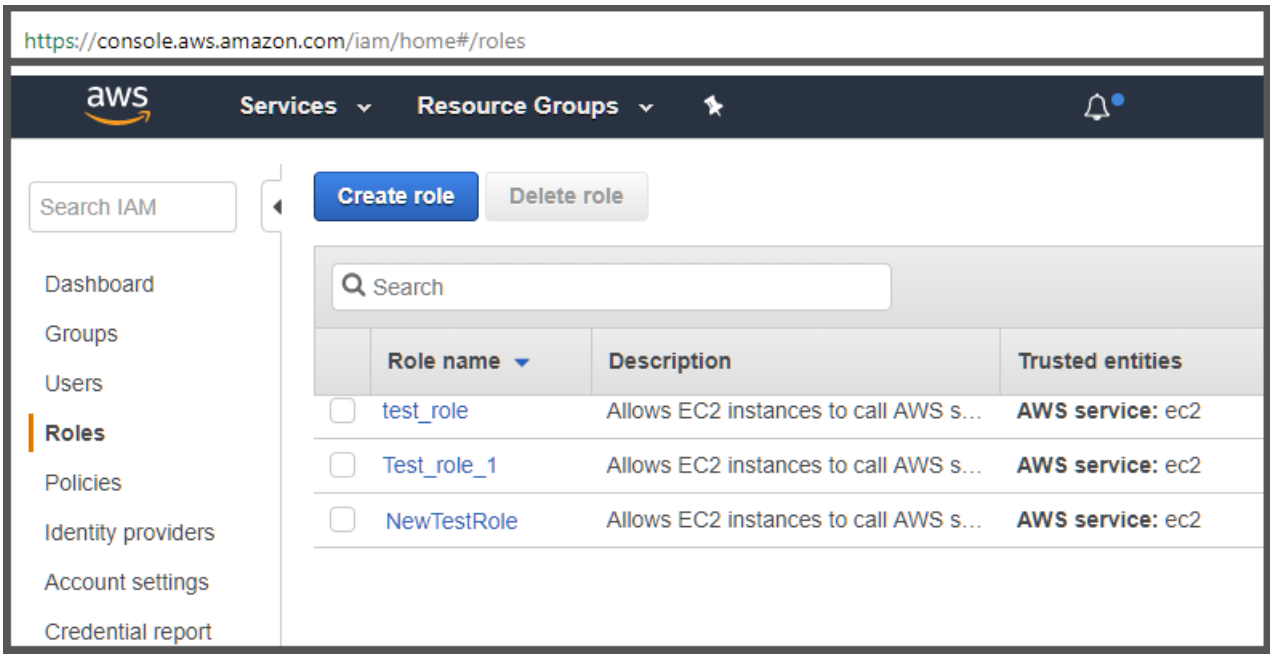
Прежде чем разворачивать Сервер администрирования, создайте в Консоли управления AWS (см. раздел AWS console - https://console.aws.amazon.com/iam) IAM-роль с необходимыми правами для установки

программ на инстансы. Подробнее см. в справке AWS об IAM-ролях (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html) и о создании IAM-ролей http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create.html.

► *Чтобы создать IAM-роль для Сервера администрирования, выполните следующие действия:*

1. Откройте Консоль управления AWS (см. раздел https://console.aws.amazon.com/iam/home#/roles) и выполните вход под своей учетной записью AWS.
2. В меню слева выберите пункт **Roles** (см. рис. ниже).
3. Нажмите на кнопку **Create Role**.
4. В отобразившемся списке сервисов выберите **EC2** и затем в списке **Select Your Use case** еще раз **EC2**.
5. Нажмите на кнопку **Далее: Права**.
6. В отобразившемся списке установите флажок (флажки):
   - Напротив пункта **AmazonEC2ReadOnlyAccess**, если вы планируете только запускать опрос облачных сегментов и не планируете устанавливать программы на инстансы EC2 с помощью AWS API.
   - Напротив пунктов **AmazonEC2ReadOnlyAccess** и **AmazonSSMFullAccess**, если вы планируете и запускать опрос облачных сегментов, и устанавливать программы на инстансы EC2 с помощью AWS API. В этом случае вам понадобится также назначить на защищаемые инстансы EC2 IAM-роль с правами AmazonEC2RoleforSSM (см. раздел "Создание IAM-роли для установки программ на инстансы Amazon EC2" на стр. 781).
7. Нажмите на кнопку **Далее: Просмотр**.
8. Введите имя и описание IAM-роли и нажмите на кнопку **Create role**.

   Созданная роль отобразится в списке ролей с именем и описанием, которые вы ввели.



Вам потребуется назначить эту роль на инстанс EC2, который вы будете использовать в качестве Сервера администрирования.

Созданная роль доступна для всех программ на Сервере администрирования. Поэтому любая программа, работающая на Сервере администрирования, имеет возможность опрашивать облачные сегменты либо устанавливать программы на инстансы EC2 внутри облачного сегмента.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

См. также:

Создание учетной записи IAM-пользователя для работы Kaspersky Security Center.....780

Шаг 3.Аутентификация в облачном окружении.....803

Создание учетной записи IAM-пользователя для работы Kaspersky Security Center

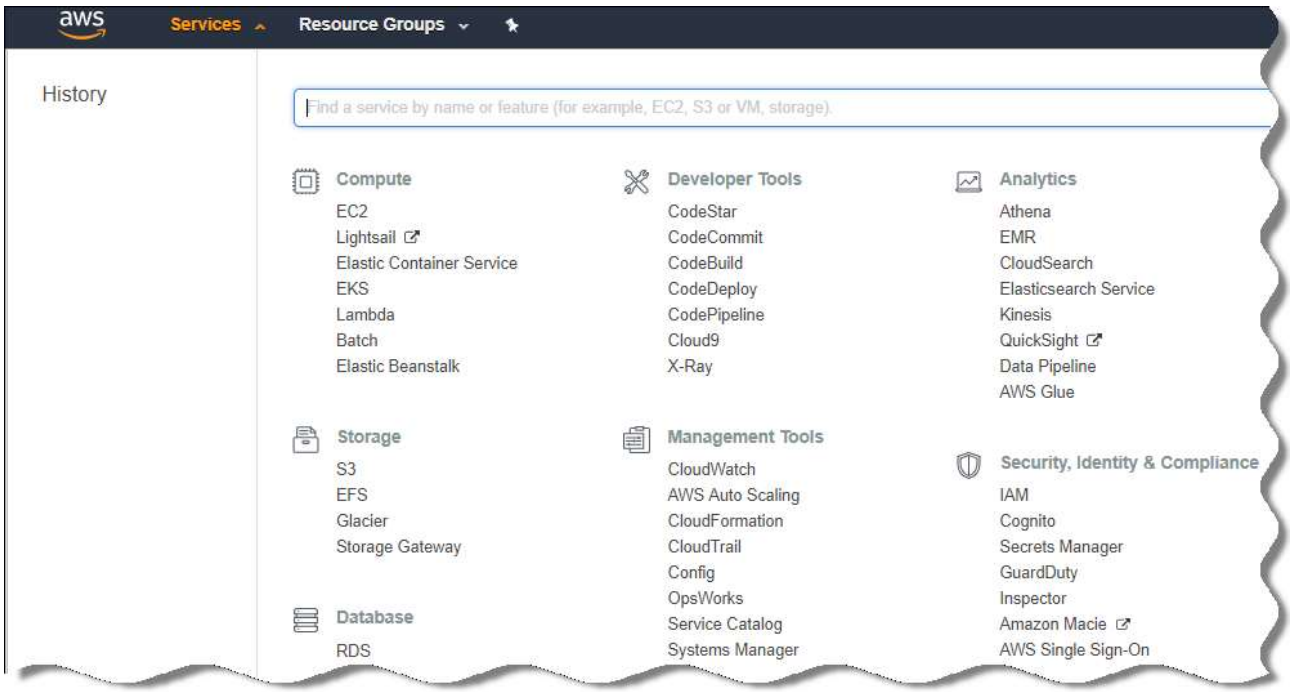
Учетная запись IAM-пользователя необходима для работы с Kaspersky Security Center, если Серверу администрирования не назначена IAM-роль с правами на обнаружение устройств и установку программ на инстансы. Эта же учетная запись или другая учетная запись также требуется для резервного копирования задачи данных Сервера администрирования, если вы используете корзину S3. Вы можете создать одну учетную запись IAM-пользователя с требуемыми правами или две разные учетные записи.

Для IAM-пользователя автоматически создается *ключ доступа IAM*, который вам потребуется предоставить Kaspersky Security Center на этапе первоначальной настройки. Ключ доступа IAM состоит из ID ключа доступа и секретного ключа. Подробнее о сервисе IAM см. на следующих справочных страницах AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.htmlhttp://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html%23UseCase_EC2http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2 http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

► *Чтобы создать учетную запись IAM-пользователя с необходимыми правами, выполните следующие действия:*

1. Откройте Консоль управления AWS (см. раздел https://console.aws.amazon.com/iam) и выполните вход под своей учетной записью AWS.
2. В списке служб AWS выберите **IAM** (как показано на рисунке ниже).



Откроется окно, содержащее список имен пользователей и меню, с помощью которого вы сможете работать с инструментом.

3. Перейдите к областям консоли, использующим учетные записи пользователей, и добавьте новое

имя пользователя или имена.

4. Для пользователей, которых вы добавили, укажите следующие параметры AWS:
   - Тип доступа: **Programmatic Access**.
   - Границы разрешений не установлены.
   - Разрешения:
     - **ReadOnlyAccess** - если вы планируете только запускать опрос облачных сегментов и не планируете устанавливать программы на инстансы EC2 с помощью AWS API;
     - **ReadOnlyAccess** и **AmazonSSMFullAccess** – если вы планируете и запускать опрос облачных сегментов, и устанавливать программы на инстансы EC2 с помощью AWS API. В этом случае вы должны назначить защищаемым инстансам EC2 IAM-роль с правами AmazonEC2RoleforSSM (см. раздел "Создание IAM-роли для установки программ на инстансы Amazon EC2" на стр. 781).

     После добавления разрешений внимательно их просмотрите. В случае ошибки выбора параметров перейдите к предыдущему экрану и выполните выбор параметров снова.
5. После того как вы создали учетную запись, отобразится таблица с ключом доступа IAM нового IAM-пользователя. ID ключа доступа отобразится в графе **Access key ID**. Секретный ключ отобразится в графе **Secret access key** в виде звездочек. Чтобы посмотреть секретный ключ, нажмите **Show**.

Созданная учетная запись отобразится в списке учетных записей IAM-пользователей, соответствующих вашей учетной записи в AWS.

При развертывании Kaspersky Security Center в облачном сегменте вам потребуется указать, что вы пользуетесь учетной записью IAM-пользователя, и предоставить Kaspersky Security Center ключ доступа и секретный ключ доступа.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

См. также:

Создание IAM-роли для Сервера администрирования.....777

Шаг 3.Аутентификация в облачном окружении.....803

Создание IAM-роли для установки программ на инстансы Amazon EC2

Прежде чем разворачивать защиту на инстансах EC2 средствами Kaspersky Security Center, создайте в Консоли управления AWS (см. раздел https://console.aws.amazon.com/iam) IAM-роль с необходимыми правами для установки программ на инстансы. Подробнее см. в справке AWS об IAM-ролях (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html) и о создании IAM-ролей

(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create.html).

IAM-роль необходима для того, чтобы назначать ее на все инстансы EC2, на которые вы планируете устанавливать программы безопасности с помощью Kaspersky Security Center. Если вы не назначите инстансу IAM-роль, обладающую необходимыми правами, установка программ средствами AWS API на этот инстанс завершится с ошибкой.

Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

► *Чтобы создать IAM-роль для установки программ на инстансы, выполните следующие действия:*

1. Откройте Консоль управления AWS (см. раздел https://console.aws.amazon.com/iam/home#/roles) и выполните вход под своей учетной записью AWS.
2. В меню слева выберите пункт **Roles**.
3. Нажмите на кнопку **Create Role**.
4. В отобразившемся списке сервисов выберите **EC2** и затем в списке **Select Your Use case** еще раз **EC2**.
5. Нажмите на кнопку **Далее: Права**.
6. В отобразившемся списке установите флажок напротив пункта **AmazonEC2RoleforSSM**.
7. Нажмите на кнопку **Далее: Просмотр**.
8. Введите имя и описание IAM-роли и нажмите на кнопку **Create role**.

   Созданная роль отобразится в списке ролей с именем и описанием, которые вы ввели.

В дальнейшем вы можете использовать созданную IAM-роль при создании новых инстансов EC2, которые вы будете защищать с помощью Kaspersky Security Center, а также ассоциировать ее с уже существующими инстансами.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Работа с Amazon RDS

В этом разделе описывается, какие действия необходимо выполнить, чтобы подготовить базу данных Amazon Relational Database Service (RDS) для Kaspersky Security Center, поместить ее в группу параметров, создать IAM-роль для работы с базой данных RDS, подготовить корзину S3 для хранения данных и перенести базу данных в существующую базу данных RDS.

Amazon Relational Database Service (Amazon RDS) это веб-сервис, который помогает пользователям AWS настраивать, управлять и масштабировать реляционную базу данных в облачном окружении AWS. Вы можете использовать базу данных Amazon RDS для работы с Kaspersky Security Center.

В этом разделе

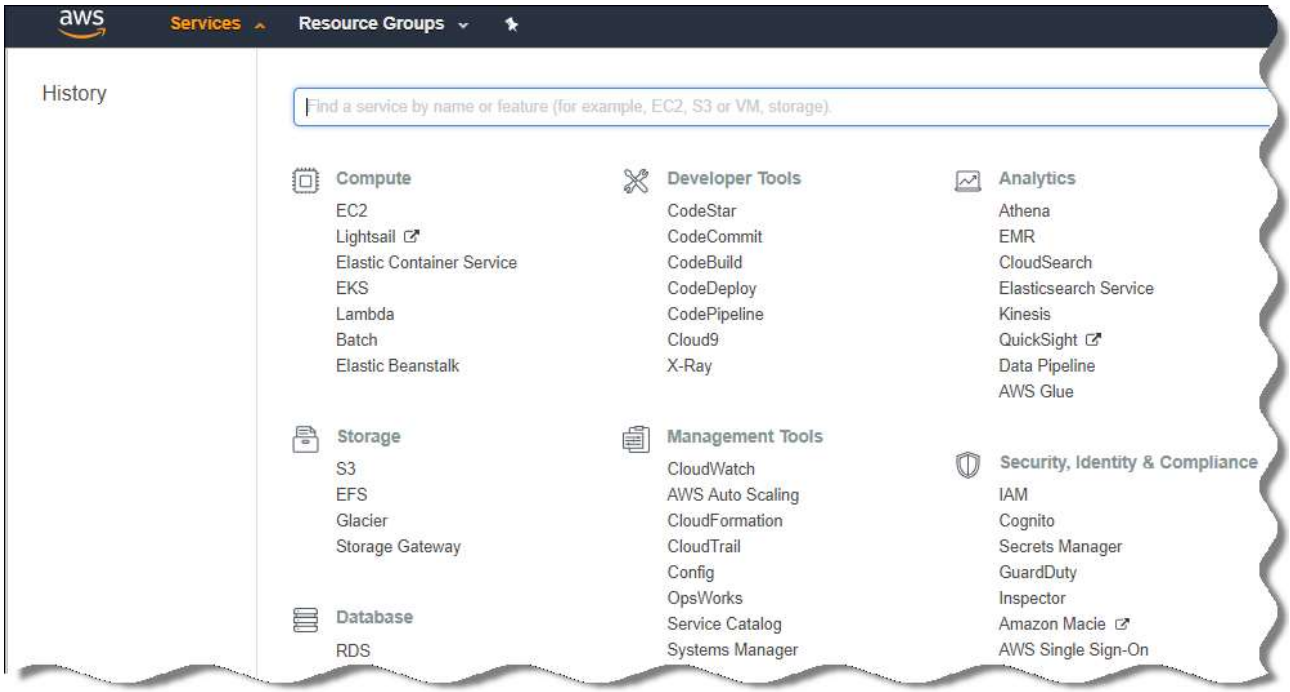
Создание инстанса Amazon RDS

Если вы хотите использовать Amazon RDS в качестве СУБД, вы можете создать инстанс базы данных Amazon RDS.

► *Чтобы создать инстанс базы данных Amazon RDS, выполните следующие действия:*

1. Откройте Консоль управления AWS https://console.aws.amazon.com https://console.aws.amazon.com и войдите под своей учетной записью.
2. В меню выберите пункт **Службы**.

   Отобразится список доступных служб (см. рис. ниже).



3. В списке выберите **RDS**.
4. На открывшейся странице нажмите на кнопку **Launch a DB instance** (в разделе **Create instance**).

5. Используя интерфейс AWS, создайте базу данных со следующими параметрами:

   - Ядро: Microsoft SQL Server, SQL Express Edition.

     Этот вариант был протестирован, но вы можете выбрать другую версию Microsoft SQL Server Edition. Если вы выбираете другую версию Microsoft SQL Server Edition, вы должны выбрать другую версию ядра СУБД.

   - Версия ядра СУБД: SQL Server 2014 12.00.5546.0v1.
   - Класс экземпляра СУБД: db.t2.medium.
   - Тип хранилища: General purpose.
   - Размер хранилища: минимум 50 ГБ.
   - Группа безопасности: та же группа, в которую входит инстанс EC2 с установленным Сервером администрирования Kaspersky Security Center.

   Создайте идентификатор, имя пользователя и пароль для экземпляра RDS.

   Вы можете оставить значения всех параметров по умолчанию. Или измените значения параметров, заданных по умолчанию, если вы хотите настроить инстанс Amazon RDS. Подробную информацию смотрите на справочных страницах AWS.

6. На последнем шаге AWS отображает результат процесса. Если вы хотите просмотреть подробную информацию инстанса Amazon RDS, нажмите на **View DB instance details**. Если вы хотите перейти к следующему действию, создайте группы параметров для инстанса Amazon RDS (см. раздел "Создайте группы параметров для инстанса Amazon RDS" на стр. 784).

Создание инстанса Amazon RDS занимает несколько минут. После того как инстанс создан, вы можете использовать его для работы с данными Kaspersky Security Center.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

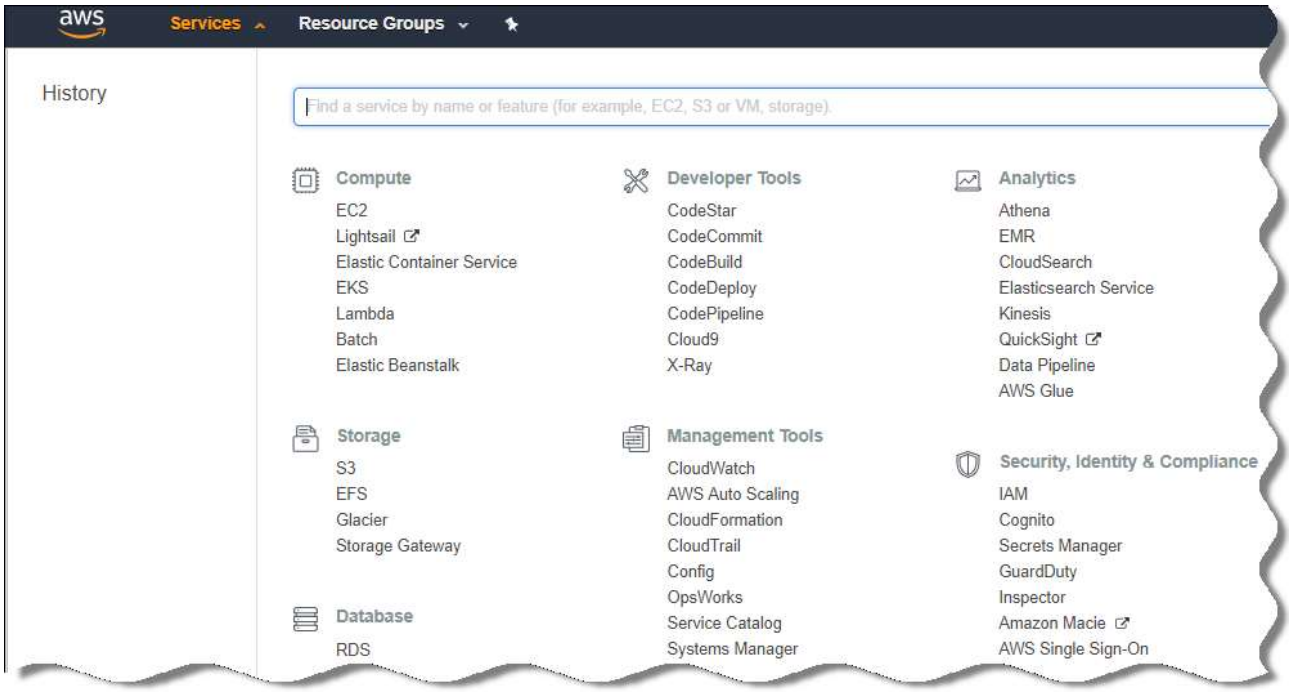
Создание группы параметров для инстанса Amazon RDS

Вам нужно поместить инстанс Amazon RDS в группу параметров.

► *Чтобы создать группу параметров для инстанса Amazon RDS, выполните следующие действия:*

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью.
2. В меню выберите пункт **Службы**.

Отобразится список доступных служб (см. рис. ниже).



3. В списке выберите **RDS**.
4. В левой панели нажмите на **Option groups**.
5. Нажмите на кнопку **Create group**.
6. Создайте группу параметров со следующими параметрами, если вы выбрали SQL Server на шаге создания инстанса Amazon RDS (см. раздел "Создание инстанса Amazon RDS" на стр. 783):
   - Ядро: SQLserver-ex.
   - Основная версия ядра: 12.00.

   Если вы выбрали базу данных, отличную от SQL, на этапе создания инстанса Amazon RDS, выберите соответствующее ядро.

Группа параметров создана. Созданная группа параметров отображается в списке.

После создания группы параметров поместите инстанс Amazon RDS в эту группу параметров.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

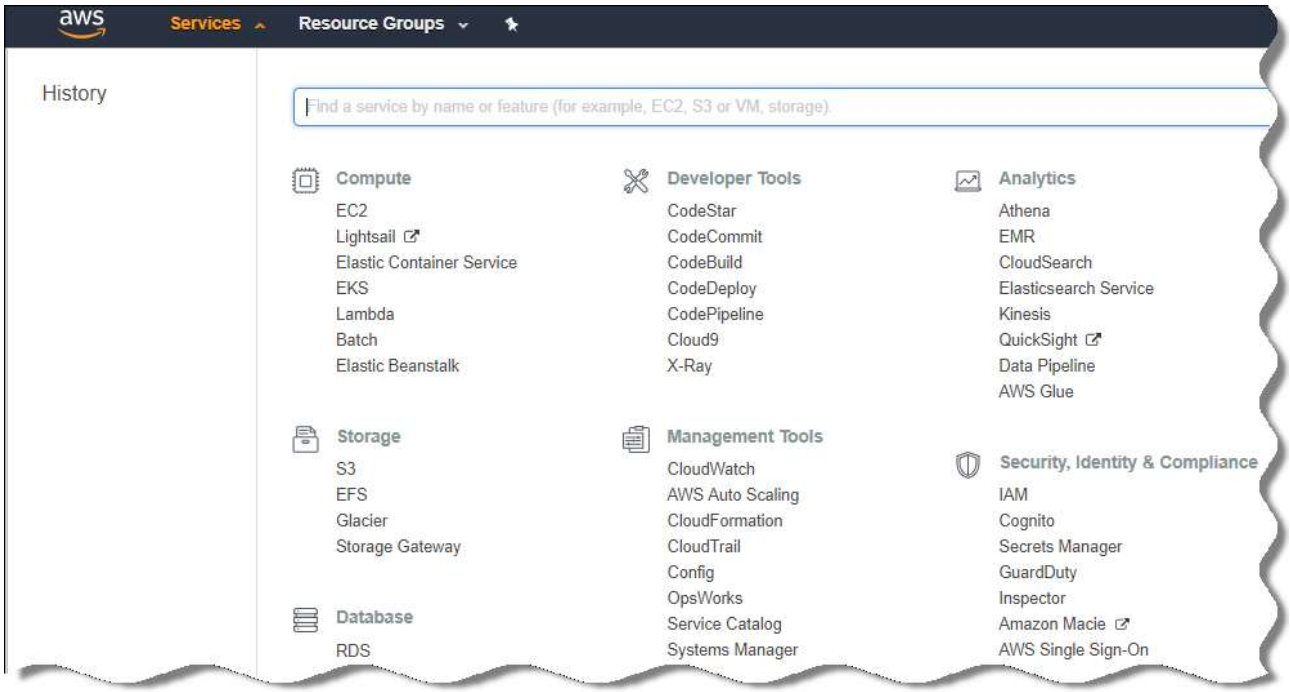
Изменение группы параметров

Заданная по умолчанию конфигурация группы параметров, в которую вы поместили инстанс Amazon RDS, не достаточна для работы с базой данных Kaspersky Security Center. Необходимо добавить параметр в группу параметров и создать IAM-роль для работы с базой данных.

► *Чтобы изменить группу параметров и создать IAM-роль, выполните следующие действия:*

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью.
2. В меню выберите пункт **Службы**.

   Отобразится список доступных служб (см. рис. ниже).



3. В списке выберите RDS.
4. В левой панели нажмите на **Option groups**.

   Отобразится список групп параметров.
5. Выберите группу параметров, в которую вы поместили инстанс Amazon RDS, и нажмите на кнопку **Добавить параметр**.

   Откроется окно **Добавить параметр**.
6. В разделе IAM-роль выберите параметр **Create a new role** / **Yes** и введите имя новой IAM-роли.

   Роль создана с набором прав по умолчанию. Позже вы можете изменить эти права (см. раздел "Изменение прав IAM-роли для инстанса базы данных Amazon RDS" на стр. 787).
7. В разделе корзины S3 выполните одно из следующих действий:
   - Если инстанс корзины Amazon S3 для резервной копии не создан, перейдите по ссылке **Создать корзину S3** и создайте корзину S3, используя интерфейс AWS(см. раздел "Подготовка корзины S3 Amazon для базы данных" на стр. 787).
   - Если вы уже создали инстанс корзины Amazon S3 для резервной копии данных Сервера администрирования, выберите требуемую корзину S3 из раскрывающегося меню.
8. Чтобы завершить добавление параметров, нажмите на кнопку **Добавить параметр** в нижней части

страницы.

Вы изменили группу параметров и создали IAM-роль для работы с базы данных RDS.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Изменение прав IAM-роли для инстанса базы данных Amazon RDS

После того, как вы добавили параметры в группу параметров(см. раздел "Изменение группы параметров" на стр. 785), вам необходимо назначить требуемые права IAM-роли, созданной для работы с инстансом базы данных Amazon RDS.

► *Чтобы назначить требуемые права IAM-роли, которую вы создали для работы с инстансом базы данных Amazon RDS, выполните следующие действия:*

1. Убедитесь, что Консоль управления AWS (https://console.aws.amazon.com https://console.aws.amazon.com) открыта и вы вошли под вашей учетной записью.
2. В списке служб выберите **IAM**.

   Откроется окно, содержащее список имен пользователей и меню, с помощью которого вы сможете работать с инструментом.
3. В меню выберите **Роли**.
4. В списке IAM-ролей выберите роль, которую вы создали во время добавления параметров в группу параметров (см. раздел "Изменение группы параметров" на стр. 785).
5. Используя интерфейс AWS, удалите политику **sqlNativeBackup-<date>**.
6. Используя интерфейс AWS назначьте политику **AmazonS3FullAccess** роли.

IAM-роль получает требуемые права для работы с Amazon RDS.

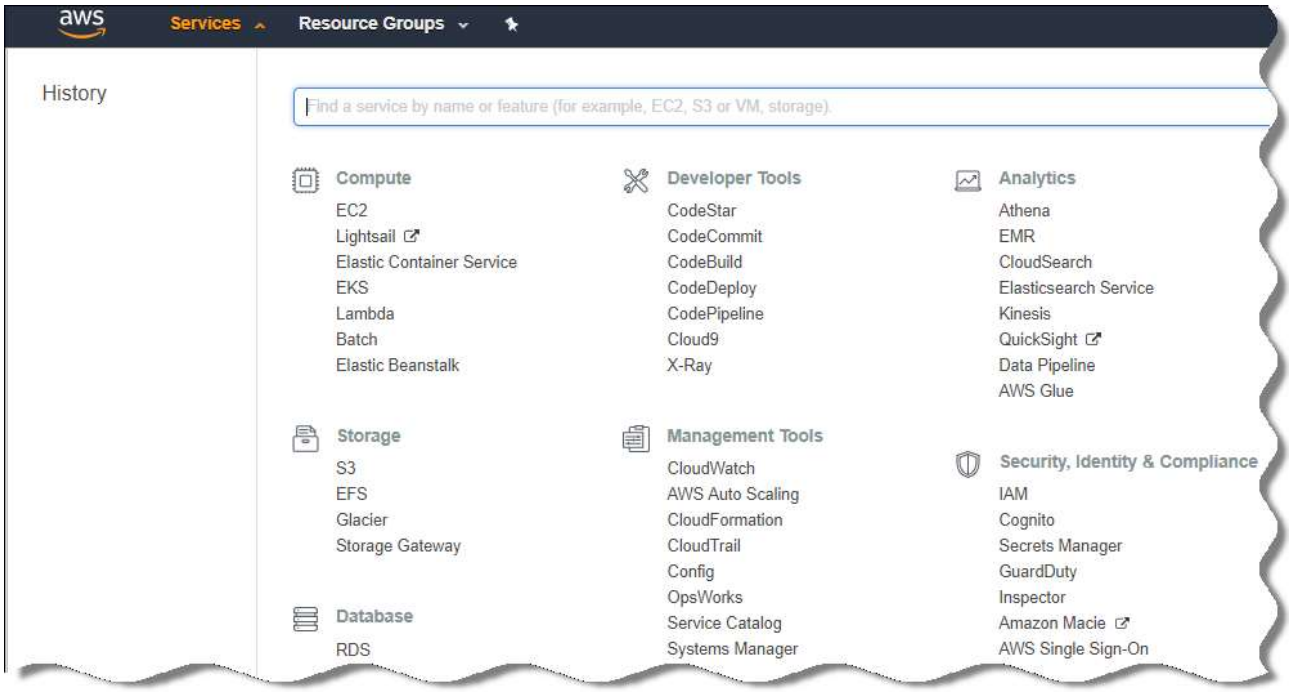
Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Подготовка корзины S3 Amazon для базы данных

Если вы планируете использовать базу данных Amazon Relational Database System (Amazon RDS), вам потребуется создать инстанс корзины Buzz Amazon Simple Storage Service (Amazon S3), в котором будет храниться обычная резервная копия данных. Подробную информацию об Amazon S3 и корзинах S3 см. в справке Amazon. Подробную информацию о создании инстанса Amazon S3, см. в справке Amazon S3 (https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-bucket.html).

► *Чтобы создать корзину Amazon S3, выполните следующие действия:*

1. Убедитесь, что Консоль управления AWS https://console.aws.amazon.com/ открыта и вы вошли под вашей учетной записью.
2. В списке служб AWS выберите S3.



3. Перейдите в консоль, чтобы создать корзину, и следуйте далее указаниям мастера.
4. Выберите такой же регион, в котором расположен ваш Сервер администрирования (или будет расположен).
5. На последнем шаге убедитесь, что новая корзина появилась в списке корзин.

Корзина S3 создана и отображается в списке корзин. Вы можете указать корзину при добавлении параметра в группу параметров (см. раздел "Изменение группы параметров" на стр. 785). Вы можете также указать адрес вашей корзины S3 в Kaspersky Security Center при создании задачи Резервное копирование данных Сервера администрирования в Kaspersky Security Center(см. раздел "Шаг 7.Создание первоначальной конфигурации защиты" на стр. 808).

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

См. также:

Параметры базы данных для работы в облачном окружении 774

Перенос базы данных в Amazon RDS

Вы можете перенести вашу базу данных Kaspersky Security Center с локального устройства на инстанс Amazon S3, который поддерживает Amazon RDS. Для этого вам необходимы корзина S3 (см. раздел "Подготовка корзины S3 Amazon для базы данных" на стр. 787) для базы данных RDS и учетная запись IAM-пользователя с правами AmazonS3FullAccess для этой корзины S3 (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

► *Чтобы перенести базу данных, выполните следующие действия:*

1. Убедитесь, что вы создали инстанс RDS (см. раздел "Создание инстанса Amazon RDS" на стр. 783) (подробную информацию см. на справочных страницах Amazon RDS https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html).
2. На вашем физическом Сервере администрирования (локальном), запустите утилиту резервного копирования для данных Сервера администрирования.
3. Скопируйте резервную копию данных на инстанс EC2, на котором установлен Сервер администрирования.

   Убедитесь, что на инстансе EC2, на котором установлен Сервер администрирования, достаточно свободного дискового пространства. В окружении AWS вы можете добавить дисковое пространство для вашего инстанса, чтобы выполнить процесс переноса базы данных.

4. Снова запустите утилиту резервного копирования в неинтерактивном режиме на Сервере администрирования в AWS (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. 566).

   В результате запустится мастер резервного копирования и восстановления данных.

5. На шаге **Выбор действия** выберите пункт **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.
6. На шаге **Параметры восстановления** нажмите на кнопку **Обзор** рядом с полем **Папка для хранения резервных копий**.
7. В открывшемся окне **Вход в онлайн-хранилище** заполните следующие поля и нажмите на кнопку **ОК**:

   - **Имя корзины S3**

     Имя корзины Amazon S3 (см. раздел "Подготовка корзины S3 Amazon для базы данных" на стр. 787).

   - **Хранилище резервных копий**

     Укажите расположение папки, предназначенной для хранения резервных копий.

   - **ID ключа доступа**

     Ключ доступа AWS IAM, принадлежащий IAM-пользователю с правами

использования корзины Amazon S3 (права AmazonS3FullAccess).

- **Секретный ключ**

  Секретный ключ AWS IAM, принадлежащий IAM-пользователю с правами использования корзины Amazon S3 (права AmazonS3FullAccess).

8. Выберите параметр **Перенести из локальной резервной копии данных**. Станет доступна кнопка **Обзор**.
9. Нажмите на кнопку **Обзор** и выберите на Сервере администрирования AWS папку, в которую вы поместили файл резервной копии данных.
10. Нажмите на кнопку **Далее** и завершите процедуру.

Данные будут храниться в базе данных RDS с использованием корзины S3. Вы можете использовать эту базу данных для дальнейшей работы с Kaspersky Security Center в окружении AWS.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Работа в облачном окружении Microsoft Azure

В этом разделе представлена информация о том, как развернуть и поддерживать Kaspersky Security Center в облачном окружении, предоставленном платформой Amazon Web Services, и как развернуть защиту на виртуальных машинах внутри облачного окружения.

В Kaspersky Security Center, который был развернут с использованием подписки с ежемесячной тарификацией в зависимости от объема услуг, возможности Системного администрирования активируются автоматически, но Управление мобильными устройствами не может быть активировано.

Адреса веб-страниц в этом документе приведены по состоянию на сентябрь 2018 года.

В этом разделе

О работе в Microsoft Azure

Чтобы работать с платформой Microsoft Azure, в частности для покупки программ на Azure Marketplace и создания виртуальных машин, вам потребуется подписка Azure. Перед развертыванием Сервера администрирования создайте ID приложения в Azure с правами, необходимыми для установки программ на виртуальные машины.

Если вы приобрели образ Kaspersky Security Center на Azure Marketplace, вы можете развернуть виртуальную машину с готовым образом AMI Сервера администрирования Kaspersky Security Center. Вы должны выбрать параметры виртуальной машины, но вам не нужно устанавливать программы самостоятельно. После установки вы можете запустить Консоль администрирования и подключиться к Серверу администрирования, чтобы начать работу с Kaspersky Security Center.

Вы также можете использовать виртуальную машину Azure с развернутым на нем Сервером администрирования Kaspersky Security Center для защиты физических устройств (например, если такой облачный сервер оказывается выгоднее в обслуживании и содержании, чем физический). В этом случае работа с Сервером администрирования будет устроена так же, как если бы Сервер администрирования был установлен на физическом устройстве. Если вы не планируете использовать инструменты Azure API, ID приложения в Azure вам не нужен. В этом случае подписки Azure достаточно.

Создание подписки, идентификатора приложения и пароля

Для работы с Kaspersky Security Center в окружении Microsoft Azure вам нужны подписка Azure, ID

приложения в Azure и пароль приложения в Azure. Вы можете использовать существующую подписку, если у вас она уже есть.

Подписка на Azure предоставляет владельцу доступ к Microsoft Azure Platform Management Portal и сервисам Microsoft Azure. Владелец может использовать Microsoft Azure Platform, чтобы управлять службами, такими как Azure SQL и Azure Storage.

► *Чтобы создать подписку Microsoft Azure,*

перейдите по ссылке https://account.windowsazure.com/Subscriptions и следуйте инструкциям.

Подробная информация о создании подписки доступна на сайте Microsoft https://docs.microsoft.com/en-us/partner-center/create-a-new-subscription. Вы получите идентификатор подписки, который затем предоставите Kaspersky Security Center вместе с ID приложения и паролем (см. раздел "Шаг 3. Аутентификация в облачном окружении" на стр. 803).

► *Чтобы создать и сохранить ID приложения и пароль Azure, выполните следующие действия:*

1. Перейдите по ссылке https://portal.azure.com https://portal.azure.com и убедитесь, что выполнили вход.
2. Следуя инструкциям на странице справки https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal, создайте ID приложения.
3. В свойствах программы перейдите в раздел **Keys**.
4. В разделе **Keys** заполните поля **Description** и **Expires** и оставьте поле **Value** пустым.
5. Нажмите на кнопку **Сохранить**.

   После того как вы нажмете на кнопку **Save**, система автоматически заполнит поле **Value** длинной последовательностью символов. Эта последовательность символов является вашим паролем приложения в Azure (например, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Описание отображается так, как вы его указали.
6. Скопируйте пароль и сохраните его, чтобы позже вы смогли предоставить ID приложения и пароль в Kaspersky Security Center (см. раздел "Шаг 3. Аутентификация в облачном окружении" на стр. 803).

   Вы можете скопировать пароль только при его создании. Позже пароль больше не будет отображаться, и вы не сможете его восстановить.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Назначение роли для ID приложения в Azure

Если требуется только обнаружить виртуальные машины с помощью процесса обнаружения устройств, ID приложения в Azure должна быть назначена роль Читатель (Reader). Если требуется не только обнаружить виртуальные машины, но и развернуть защиту на виртуальных машинах, вашему ID приложения в Azure должна быть назначена роль Участник виртуальных машин (Virtual Machine Contributor).

Следуйте инструкциям, приведенным на веб-сайте Microsoft, чтобы назначить роль для ID приложения в Azure.

Развертывание Сервера администрирования в Microsoft Azure и выбор базы данных

► *Чтобы развернуть Сервер администрирования в окружении Microsoft Azure, выполните следующие действия:*

1. Войдите в Microsoft Azure, используя свою учетную запись.
2. Перейдите на портал Azure https://portal.azure.com/#create/.
3. В левой части панели нажмите на зеленый значок плюса.
4. Напишите "Kaspersky Hybrid Cloud Security" в поле поиска меню.

   Kaspersky Hybrid Cloud Security – это комбинация Kaspersky Security Center и двух программ безопасности для защиты инстансов: Kaspersky Endpoint Security для Linux и Kaspersky Security для Windows Server.
5. В списке результатов выберите Kaspersky Hybrid Cloud Security или Kaspersky Hybrid Cloud Security (BYOL).

   В правой части экрана отобразится информационное окно.
6. Прочитайте информацию и нажмите на кнопку Создать в информационном окне.
7. Заполните требуемые поля. Используйте подсказки и справку, чтобы получить информацию и помощь.
8. При выборе размера выберите один из трех параметров.

   В большинстве случаев 8 ГБ оперативной памяти достаточно. В Azure вы можете увеличить размер оперативной памяти и других ресурсов на виртуальной машине в любое время.
9. При выборе базы данных выберите один из следующих вариантов, в соответствии с вашим планом (см. раздел "Параметры базы данных для работы в облачном окружении" на стр. 774):

   - Локальная. Если вам нужна база данных на той же виртуальной машине, на которой будет развернут Сервер администрирования. Kaspersky Security Center поставляется с базой данных SQL Server Express. Выберите этот параметр, если базы данных SQL Server Express достаточно для ваших потребностей.
   - Новая. Если вы хотите создать новую базу данных RDS в окружении Azure. выберите этот параметр, если вы хотите использовать СУБД, отличную от SQL Server Express. Ваши данные

будут перенесены в облачное окружение, где они останутся, и у вас не будет никаких дополнительных затрат.

- Существующая. Если вы хотите использовать существующий сервер базы данных. В этом случае вы должны указать его месторасположение. Если сервер вне окружения Azure, ваши данные будут перенесены через интернет, что может привести к дополнительным расходам.

10. При вводе идентификатора подписки используйте подписку, созданную ранее (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

После развертывания вы можете подключиться к Серверу администрирования с помощью RDP. Вы можете использовать Консоль администрирования для работы с Сервером администрирования.

Работа с Azure SQL

В этом разделе описаны действия, необходимые для подготовки базы данных Microsoft Azure к использованию Kaspersky Security Center, а также для подготовки учетной записи хранения Azure и переноса существующей базы данных в Azure SQL.

База данных SQL это универсальная служба управления реляционными базами данных в Microsoft Azure.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

В этом разделе

Создание учетной записи хранения Azure

В Microsoft Azure требуется создать учетную запись хранения для работы с базой данных Azure SQL и для скриптов развертывания.

► *Чтобы создать учетную запись хранения, выполните следующие действия:*

1. Выполните вход на портал Azure.
2. В левой панели выберите пункт **Учетные записи хранения** и перейдите в окно **Учетные записи хранения**.
3. В окне **Учетные записи хранения** нажмите на кнопку **Добавить**, чтобы перейти в окно **Создание**

учетной записи хранения.

4. Заполните все необходимые поля для создания учетной записи хранения:
   - Местоположение: должно совпадать с местоположением (географическим регионом) Сервера администрирования.
   - Прочие поля: можно оставить указанные по умолчанию значения.

   Используйте подсказки, чтобы получить информацию о каждом поле.

   После создания учетной записи хранения отобразится список ваших учетных записей хранения.
5. В списке учетных записей хранения выделите созданную учетную запись, чтобы посмотреть информацию о ней.
6. Убедитесь, что вам известны имя учетной записи, группа ресурсов и ключи доступа для этой учетной записи хранения. Эти данные понадобятся вам при работе с Kaspersky Security Center.

Справку можно посмотреть на веб-сайте Azure.

Если у вас уже есть учетная запись хранения, ее можно использовать для работы с Kaspersky Security Center.

Создание базы данных Azure SQL и SQL-сервера

В окружении Azure вам понадобится база данных SQL и SQL-сервер.

► *Чтобы создать базу данных Azure SQL и SQL-сервер, выполните следующие действия:*

1. Выполните инструкции, приведенные на веб-сайте Azure.

   Вы можете создать новый сервер, когда появится приглашение от Microsoft Azure. Если у вас уже есть Azure SQL Server, вы можете использовать его для Kaspersky Security Center, а не создавать новый сервер.
2. После создания базы данных SQL и SQL-сервера убедитесь, что вам известны имя ресурса и группа ресурсов.
   a. Перейдите по ссылке https://portal.azure.com https://portal.azure.com и убедитесь, что выполнили вход.
   b. На левой панели выберите пункт **Базы данных SQL**.
   c. Выберите имя базы данных в списке баз данных.

      Откроется окно свойств политики.
   d. Имя базы данных является именем ресурса. Имя группы ресурсов отображается в окне свойств в разделе **Обзор**.

Имя ресурса и группа ресурсов базы данных понадобятся вам при переносе базы данных в Azure SQL (см. стр. 796).

Перенос базы данных в Azure SQL

После развертывания Сервера администрирования в окружении Microsoft Azure (см. раздел "Развертывание Сервера администрирования в Microsoft Azure и выбор базы данных" на стр. 793) можно выполнить перенос базы данных Kaspersky Security Center с физического устройства в Azure SQL. Для использования базы данных Azure SQL необходима учетная запись хранения Azure. Также у вас должен быть Microsoft SQL Server и Платформа приложения уровня данных (DacFx) и SQLSysCLRTypes на вашем Сервере администрирования.

► *Чтобы перенести базу данных, выполните следующие действия:*

1. Убедитесь, что вы создали учетную запись хранения Azure (см. раздел "Создание учетной записи хранения Azure" на стр. 794).
2. Убедитесь, что на Сервере администрирования есть DacFx и SQLSysCLRTypes.

   Вы можете загрузить Microsoft SQL Server и Платформу приложения уровня данных (17.0.1 DacFx) с официального сайта Microsoft: https://www.microsoft.com/ru-ru/download/details.aspx?id=55114. Дополнительную информацию см. в приведенной инструкции.

   Вы можете загрузить SQLSysCLRTypes с официального сайта Microsoft. Выберите версию, соответствующую версии вашего сервера SQL:

   - Пакет дополнительных компонентов для Microsoft SQL Server 2012 с пакетом обновления 3 (SP3)
   - Пакет дополнительных компонентов для Microsoft SQL Server 2014
   - Пакет дополнительных компонентов для Microsoft SQL Server 2016 https://www.microsoft.com/en-us/download/details.aspx?id=52676
   - Пакет дополнительных компонентов для Microsoft SQL Server 2017

   Дополнительные сведения см. на веб-странице соответствующей программы.
3. На вашем физическом Сервере администрирования запустите утилиту резервного копирования "Лаборатории Касперского" для данных Сервера администрирования с включенным параметром **Перенос в формат Azure**.
4. Поместите файл резервной копии данных на Сервер администрирования в Azure.

   Убедитесь, что на виртуальной машине Azure, на которой установлен Сервер администрирования, достаточно свободного дискового пространства. В окружении Azure можно добавить дисковое пространство для виртуальной машины, чтобы обеспечить процесс переноса базы данных.
5. На Сервере администрирования, расположенного в облачном окружении Microsoft Azure, еще раз запустите утилиту резервного копирования "Лаборатории Касперского" в интерактивном режиме (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. 566).

   В результате запустится мастер резервного копирования и восстановления данных.

6. На шаге **Выбор действия** выберите пункт **Выполнить восстановление данных Сервера администрирования** и нажмите на кнопку **Далее**.
7. На шаге **Параметры восстановления** нажмите на кнопку **Обзор** рядом с полем **Папка для хранения резервных копий**.
8. В открывшемся окне **Вход в онлайн-хранилище** заполните следующие поля и нажмите на кнопку **ОК**:

   - **Имя учетной записи хранения Azure**

     Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center (см. раздел "Создание учетной записи хранения Azure" на стр. 794).

   - **Хранилище резервных копий**

     Укажите расположение папки, предназначенной для хранения резервных копий.

   - **Идентификатор подписки Azure**

     Вы создали подписку на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

   - **Пароль приложения в Azure**

     Вы получили пароль к идентификатору приложения при создании ID приложения в Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

     Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

   - **Ключ доступа хранилища Azure**

     Доступен в свойствах учетной записи хранения в разделе "Access Keys" (см. раздел "Работа с Azure SQL" на стр. 794). Вы можете использовать любой ключ (key1 или key2).

   - **Имя SQL-сервера Azure**

     Доступно в свойствах SQL-сервера Azure (см. раздел "Создание базы данных Azure SQL и SQL-сервера" на стр. 795).

   - **Группа источника SQL-сервера Azure**

     Доступно в свойствах SQL-сервера Azure (см. раздел "Создание базы данных Azure SQL и SQL-сервера" на стр. 795).

   - **Идентификатор приложения в Azure**

     Вы создали этот идентификатор приложения на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

     Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны

сначала удалить первый сегмент в существующем соединении Azure.

9. Выберите параметр **Перенести из локальной резервной копии данных**.

   Станет доступна кнопка **Обзор**.

10. Нажмите на кнопку **Обзор** и выберите на Сервере администрирования в Azure папку, в которую вы поместили файл резервной копии данных.

11. Нажмите на кнопку **Далее** и завершите процедуру.

Данные будут восстановлены в базу данных Azure SQL с использованием хранилища Azure. Вы можете использовать эту базу данных для дальнейшей работы с Kaspersky Security Center в окружении Azure.

Адреса веб-страниц в этом документе приведены по состоянию на январь 2019 года.

Подготовка клиентских устройств в облачном окружении для работы с Kaspersky Security Center

Для каждого устройства, на которое вы планируете установить Сервер администрирования, Агент администрирования и программы безопасности "Лаборатории Касперского", должны быть выполнены следующие условия:

- Настройки групп безопасности делают доступными следующие порты на Сервере администрирования (минимально необходимый для развертывания набор портов):
  - 8060 HTTP – для передачи с Сервера администрирования на защищаемые инстансы инсталляционных пакетов Агента администрирования и программ безопасности;
  - 8061 HTTPS – для передачи с Сервера администрирования на защищаемые инстансы инсталляционных пакетов Агента администрирования и программ безопасности;
  - 13000 TCP – для передачи с защищаемых инстансов и подчиненных Серверов администрирования на главный Сервер администрирования с помощью SSL;
  - 13000 UDP – для передачи на Сервер администрирования информации о выключении инстансов;
  - 14000 TCP – для передачи с защищаемых инстансов и подчиненных Серверов администрирования на главный Сервер администрирования без SSL;
  - 13291 – для подключения Консоли администрирования к Серверу администрирования;
  - 40080 – для работы скриптов развертывания.

  Вы можете настроить группы безопасности в Консоли управления AWS или на портале Azure. Если вы планируете использовать Kaspersky Security Center в конфигурации, отличной от настроек по умолчанию, см. страницу справки https://support.kaspersky.com/9297#block1 https://support.kaspersky.com/9297#block1. Примеры конфигураций, отличных от конфигураций по умолчанию, не включают установку Консоли администрирования на устройстве с Сервером администрирования, но включают установку на вашу рабочую станцию или использование прокси-сервера KSN.
- На клиентских устройствах доступен порт 15000 UDP (для приема запросов на связь с Сервером администрирования).
- В облачном окружении AWS:
  - Если вы планируете использовать API AWS, задается IAM-роль, под которой будут устанавливаться программы на инстансах (см. раздел "Создание IAM-роли для установки программ на инстансы Amazon EC2" на стр. 781).
  - На каждом инстансе Amazon EC2, Systems Manager Agent (SSM-агент) установлен и запущен.
  - SSM-агент позволяет Kaspersky Security Center автоматически устанавливать программы на устройства и группы устройств, не запрашивая каждый раз подтверждение от администратора.
  - На инстансах под управлением операционной системы Windows, развернутых из образов AMI

позже ноября 2016 года, SSM-агент установлен и работает. На все остальные устройства вам потребуется устанавливать SSM-агент самостоятельно. Подробнее об установке SSM-агента на устройства под управлением операционных систем Windows и Linux см. на странице справки AWS http://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html.

- В облачном окружении Microsoft Azure:
  - На каждой виртуальной машине Azure установлен и запущен Azure VM Agent.

    По умолчанию виртуальная машина создается с Azure VM Agent и вы не должны устанавливать или включать его вручную. Дополнительные сведения Azure VM Agent на устройствах Windows и на устройствах Linux см. страницах справки Microsoft.
  - Ваш ИД приложения в Azure имеет следующие роли (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791):
    - Читатель (обнаруживает виртуальные машины при опросе сети).
    - Virtual Machine Contributor (разворачивает защиту на виртуальных машинах).
    - SQL Server Contributor (использует базу данных SQL в облачном окружении Microsoft Azure).

    Если вы хотите выполнять все эти операции, назначьте все три роли вашему ID приложения Azure.

Мастер настройки для работы в облачном окружении

Чтобы настроить Kaspersky Security Center, используя этот мастер, у вас должны быть:

- IAM-роль, которой было предоставлено право опроса облачного сегмента (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 777), или учетная запись IAM-пользователя, которому было предоставлено право опроса облачного сегмента (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780) (для работы в облачной среде AWS);
- ИД приложения в Azure, пароль и подписка (см. раздел "Создание подписки, идентификатора

приложения и пароля" на стр. 791) (для работы в облачной среде Microsoft Azure).

Если вы не хотите использовать возможности для работы в облачном окружении (например, в случае, если вы хотите управлять защитой только физических клиентских устройств), вы можете выйти из мастера настройки для работы в облачном окружении и вручную запустить стандартный мастер первоначальной настройки Сервера администрирования (см. стр. 213).

Мастер настройки для работы в облачном окружении запускается автоматически при первом подключении через Консоль администрирования к Серверу администрирования, если вы разворачиваете Kaspersky Security Center из готового образа AMI. Вы также можете запустить мастер настройки для работы в облачном окружении вручную в любое время.

► *Чтобы запустить мастер настройки для работы в облачном окружении вручную, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи** → **Мастер настройки для работы в облачном окружении**.

Приблизительное время работы с мастером составляет около пятнадцати минут.

В этом разделе

О мастере настройки для работы в облачном окружении

Мастер позволяет настроить Kaspersky Security Center с учетом особенностей работы в облачном окружении.

Мастер создает следующие объекты:

- политику Агента администрирования с настройками по умолчанию;
- политику Kaspersky Endpoint Security для Linux;
- политику Kaspersky Security для Windows Server;
- группу администрирования и правило автоматического перемещения инстансов в эту группу администрирования;
- задачу резервного копирования данных Сервера администрирования;
- задачи установки защиты на устройства под управлением Linux и Windows;
- задачи для каждого из управляемых устройств:
  - быстрый поиск вирусов;
  - загрузку обновлений.

Если вы выбрали вариант лицензирования по модели BYOL, то мастер также активирует Kaspersky Security Center с помощью файла ключа или кода активации и помещает ключ или код активации в хранилище лицензий.

Шаг 1. Выбор способа активации программы

Если вы подписывались на один из готовых образов AMI (в магазине приложений AWS Marketplace) или используете ежемесячный счет за использование SKU (в магазине приложений AWS Marketplace), то этот шаг активации будет пропущен и мастер сразу отобразит следующий шаг.

Если вы выбрали вариант лицензирования Kaspersky Security Center по схеме BYOL, мастер предложит вам выбрать способ активации программы.

Активируйте программу с помощью кода активации или файла ключа для программы Kaspersky Security для виртуальных сред или программы Kaspersky Hybrid Cloud Security.

Вы можете активировать программу следующими способами:

- Ввести код активации.

  Запустится процесс онлайн-активации. В ходе этого процесса выполняется проверка указанного кода активации, получение и активация файла ключа.

- Указать файл ключа.

Программа проверит файл ключа и либо активирует его, если в нем содержится корректная информация, либо предложит указать другой файл ключа.

Kaspersky Security Center помещает ключ в хранилище лицензий и помечает его как автоматически распространяемый на управляемые устройства (см. раздел "Автоматическое распространение лицензионного ключа" на стр. 299).

Если вы подключаетесь к инстансу с помощью стандартной программы Microsoft Windows "Подключение к удаленному рабочему столу" (Remote Desktop Connection) или аналогичной программы, требуется указать в свойствах удаленного подключения диск физического устройства, с которого вы подключаетесь. Таким образом вы обеспечите доступ с инстанса к файлам на вашем физическом устройстве и сможете выбрать и указать файл ключа.

При работе с Kaspersky Security Center, развернутым из платного образа AMI или с использованием ежемесячных счетов за использование SKU, в хранилище лицензий нельзя добавлять ключи или коды активации.

См. также:

Варианты лицензирования в облачном окружении.....773

Шаг 2. Выбор облачного окружения

Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center: AWS или Azure.

Шаг 3. Аутентификация в облачном окружении

AWS

Если вы выбрали AWS, либо укажите, что у вас есть IAM-роль с необходимыми правами (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 777), либо предоставьте Kaspersky Security Center ключ доступа AWS IAM (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 780). Без IAM-роли или ключа доступа AWS IAM невозможен опрос облачных сегментов.

Укажите следующие параметры соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента:

- **Название соединения**

  Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

  Это имя будет также использоваться как имя группы администрирования для этих инстансов.

Если вы планируете работать в двух облачных окружениях, AWS и Azure, вы можете захотеть назвать соединение "AWS Segment".

- **Использовать AWS IAM-роль**

  Выберите этот вариант, если вы уже создали IAM-роль для работы Сервера администрирования с сервисами AWS (см. раздел "Создали IAM-роль для работы Сервера администрирования с сервисами AWS" на стр. 777).

- **Использовать учетную запись AWS IAM-пользователя**

  Выберите этот вариант, если у вас есть учетная запись IAM-пользователя с необходимыми правами (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780) и вы можете ввести ID ключа и секретный ключ.

  - **ID ключа доступа**

    ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

    Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

  - **Секретный ключ**

    Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

    Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

    Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

Соединение будет сохранено в параметрах программы. Мастер настройки для работы в облачном окружении дает возможность записать только один ключ доступа AWS IAM. Впоследствии вы можете указывать и другие соединения для управления другими облачными сегментами (см. раздел "Добавление соединений для опроса облачных сегментов" на стр. 815).

Если вы хотите устанавливать программы на инстансы средствами Kaspersky Security Center, необходимо, чтобы ваша IAM-роль (либо IAM-пользователь, учетной записи которого соответствует вводимый вами ключ), имела необходимые привилегии (см. раздел "Обеспечение прав для работы Сервера администрирования Kaspersky Security Center с AWS" на стр. 777).

Azure

Если вы выбрали Azure, укажите следующие параметры соединения, которые в дальнейшем будут

использоваться для опроса облачного сегмента:

- **Название соединения**

  Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

  Это имя будет также использоваться как имя группы администрирования для этих инстансов.

  Если вы планируете работать в обоих облачных окружениях, AWS и Azure, вы можете захотеть назвать соединение "Azure Segment".

  В Kaspersky Security Center 11 можно опрашивать только один сегмент Azure. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

- **Пароль приложения в Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center (см. раздел "Создание учетной записи хранения Azure" на стр. 794).

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

Соединение будет сохранено в параметрах программы.

Шаг 4. Настройка синхронизации с AWS и определение дальнейших действий

На этом шаге начинается опрос облачного сегмента и создается специальная группа администрирования для инстансов. Инстансы, обнаруженные при опросе, перемещаются в эту группу. Настраивается расписание опроса облачного сегмента (по умолчанию каждые 5 минут).

Также создается правило автоматического перемещения **Синхронизация с облачным окружением** (см. раздел "**Синхронизация с облачным окружением**" на стр. 825). При каждом последующем сканировании облачной сети обнаруженные виртуальные устройства будут перемещаться в соответствующую подгруппу внутри группы **Управляемые устройства\Cloud**.

На странице **Настройка синхронизации с облачным сегментом и защиты развертывания** вы можете настроить следующие параметры:

- **Синхронизировать группы администрирования со структурой облачного окружения**

  Если параметр включен, то в группе **Управляемые устройства** автоматически создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети. Инстансы и виртуальные машины, обнаруженные во время каждого сканирования облачной сети, перемещаются в группу Cloud. Структура подгрупп администрирования в этой группе соответствует структуре вашего облачного сегмента (в AWS зоны доступности и группы размещения не представлены в структуре; в Azure подсети не представлены в структуре). Устройства, не идентифицированные как инстансы в облачном окружении, находятся в группе **Нераспределенные устройства**. Такая структура групп позволяет устанавливать антивирусные программы на инстансы с помощью задач групповой установки и настраивать разные политики для разных групп.

  Если параметр выключен, то также создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети, однако в группе не создаются подгруппы, соответствующие структуре облачного сегмента. Все найденные инстансы находятся в группе администрирования **Cloud** и отображаются единым списком. Если в процессе работы с Kaspersky Security Center вам потребуется произвести синхронизацию, то вы сможете изменить свойства правила **Синхронизация с облачным окружением** и форсировать его (см. раздел "Синхронизация с облачным окружением" на стр. 825). Форсирование правила перестраивает структуру групп внутри группы Cloud так, чтобы она соответствовала структуре вашего облачного сегмента.

  По умолчанию параметр выключен.

  Если этот параметр выбран, то мастер создает задачу установки защитных программ на инстансы. После завершения работы мастера автоматически запустится мастер развертывания защиты на устройствах в ваших облачных

сегментах, и вы сможете установить на эти устройства Агент администрирования и программы безопасности.

Kaspersky Security Center может выполнить развертывание с помощью собственных инструментов. Если у вас отсутствуют права на установку программ на инстансы Amazon EC2 или виртуальные машины Azure, вы можете настроить задачу **удаленной установки** вручную (см. раздел "Установка программ на устройства в облачном окружении" на стр. 821) и указать учетную запись с необходимыми правами. В этом случае задача удаленной установки не будет работать для устройств, обнаруженных с помощью AWS API или Azure. Эта задача работает только для устройств, обнаруженных с использованием опроса Active Directory, Windows-доменов или IP-диапазонов.

Если этот параметр не выбран, то мастер развертывания защиты не запускается и задачи установки программ безопасности на инстансы не создаются. Вы можете произвести оба эти действия позже вручную.

По умолчанию выбран этот вариант.

Шаг 5. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center в автоматическом режиме будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории Касперского". Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия Kaspersky Security Network**

  Клиентские устройства под управлением Kaspersky Security Center не будут предоставлять "Лаборатории Касперского" информацию о работе установленных на них программ "Лаборатории Касперского".

"Лаборатория Касперского" рекомендует участие в Kaspersky Security Network.

Шаг 6. Настройка параметров отправки почтовых уведомлений

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе программ "Лаборатории Касперского" на виртуальных клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках программ.

Для настройки рассылки оповещений о возникающих событиях программ "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **SMTP-серверы**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. В качестве адреса может использоваться IP-адрес или имя устройства в сети Windows (NetBIOS-имя).

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят, параметры ESMTP-аутентификации недоступны.

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**. Если пробное сообщение доставлено успешно по адресам, указанным в поле **Получатели (адреса электронной почты)**, то параметры настроены правильно.

Шаг 7. Создание первоначальной конфигурации защиты

На этом шаге Kaspersky Security Center автоматически создает политики и задачи. В окне **Создание первоначальной конфигурации защиты** отображается список создаваемых программой политик и задач.

Если вы используете базу данных RDS в облачном окружении AWS, вам необходимо предоставить ключ доступа IAM к Kaspersky Security Center при создании задачи резервного копирования Сервера администрирования. В этом случае заполните следующие поля:

- **Имя корзины S3**

  Имя корзины S3, которое вы создали для резервной копии данных (см. раздел "Подготовка корзины S3 Amazon для базы данных" на стр. 787).

- **ID ключа доступа**

  Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

  Поле доступно, если вы выбрали базу данных RDS для контейнера S3.

- **Секретный ключ**

Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

Если вы используете базу данных Azure SQL в облачном окружении Azure, вам необходимо предоставить информацию о Azure SQL Server Kaspersky Security Center при создании задачи резервного копирования Сервера администрирования. В этом случае заполните следующие поля:

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center (см. раздел "Создание учетной записи хранения Azure" на стр. 794).

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

- **Пароль приложения в Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Имя SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

  Доступен в свойствах учетной записи хранения в разделе "Access Keys" (см. раздел

"Работа с Azure SQL" на стр. 794). Вы можете использовать любой ключ (key1 или key2).

Кнопка **Далее** станет доступна, когда все необходимые для минимальной конфигурации защиты политики и задачи будут созданы.

Если устройство, на котором должны выполняться задачи, не видимо в сети Сервера администрирования, задачи запускаются только тогда, когда устройство становится видимым. Если вы создаете EC2 или виртуальную машину Azure, может потребоваться некоторое время, прежде чем инстанс или виртуальная машина станут видимыми для Сервера администрирования. Если вы хотите, чтобы Агент администрирования и программы безопасности были установлены на все новые устройства как можно скорее, убедитесь (см. раздел "Шаг 5. Настройка расписания задачи" на стр. 470) что параметр **Запускать пропущенные задачи** включен для задачи **Удаленная установка программы**. В противном случае на созданные инстансы/виртуальные машины не будут уставлены Агент администрирования и программы безопасности до тех пор, пока задача не запустится в соответствии с расписанием.

Шаг 8. Выбор действия, когда требуется перезагрузка операционной системы в ходе установки

Если вы ранее выбрали (см. раздел "Шаг 4. Настройка синхронизации с AWS и определение дальнейших действий" на стр. 806) **Развернуть защиту**, вы должны выбрать действие, в случае если операционная система целевого устройства должна быть перезагружена. Если вы не выбрали параметр **Развернуть защиту**, это шаг пропускается.

Выберите, перезагружать ли инстансы, если в ходе установки программ на устройства потребуется перезагрузка операционной системы:

- **Не перезагружать устройство**

  Если выбран этот вариант, устройство не будет перезагружаться после установки программы безопасности.

- **Перезагрузить устройство**

  Если выбран этот вариант, устройство будет перезагружено после установки программы безопасности.

Если вы хотите принудительно закрыть все программы в заблокированных сеансах на инстансах перед перезагрузкой, установите флажок **Принудительно закрывать программы в заблокированных сеансах**. Если флажок не установлен, необходимо будет вручную закрыть все программы, работающие на

заблокированных инстансах.

Шаг 9. Получение обновлений Сервером администрирования

На этом шаге отображается прогресс загрузки обновлений, необходимых для корректной работы Сервера администрирования. Вы можете нажать на кнопку **Далее**, не дожидаясь окончания загрузки, чтобы перейти к завершающему окну мастера.

Мастер завершает работу.

Проверка успешности настройки

► *Чтобы проверить, что Kaspersky Security Center 11 настроен для работы в облачном окружении корректно, выполните следующие действия:*

1. Запустите Kaspersky Security Center и убедитесь, что вы можете подключиться к Серверу администрирования через Консоль администрирования.
2. В дереве консоли выберите **Управляемые устройства\Cloud**.
3. Заходя в каждую подгруппу внутри группы **Управляемые устройства\Cloud**, убедитесь, что на закладке **Устройства** отображаются все устройства каждой подгруппы.

   Если устройства не отображаются, вы можете выполнить опрос соответствующего облачного сегмента вручную, чтобы их найти (см. раздел "Опрос облачного сегмента" на стр. 813).
4. Убедитесь, что на закладке **Политики** имеются активные политики для программ:
   - Агент администрирования Kaspersky Security Center
   - Kaspersky Security для Windows Server.
   - Kaspersky Endpoint Security для Linux.

   Если политик нет в списке, вы можете создать их вручную.
5. Убедитесь, что на закладке **Задачи** присутствуют задачи:
   - **резервное копирование данных Сервера администрирования;**
   - **Задача обновления для Windows Server.**
   - **Обслуживание базы данных.**
   - **Загрузка обновлений в хранилище Сервера администрирования.**
   - **Поиск уязвимостей и требуемых обновлений.**
   - **Установить защиту для Windows.**
   - **Установить защиту для Linux.**
   - **Задача быстрого опроса Windows Server.**
   - **Быстрый опрос.**
   - **Установить обновления для Linux.**

   Если политик нет в списке, вы можете создать их вручную.

Kaspersky Security Center 11 настроен для работы в облачном окружении корректно.

Группа облачных устройств

Вы можете управлять инстансами Amazon EC2 и виртуальными машинами Azure путем объединения их по группам администрирования. На этапе первоначальной настройки Kaspersky Security Center по умолчанию создает группу администрирования **Управляемые устройства\Cloud** и облачные устройства, обнаруженные во время опроса сети, перемещаются в эту группу.

Если вы установили флажок **Синхронизировать группы администрирования со структурой облачного сегмента** во время настройки синхронизации, то структура подгрупп в этой группе администрирования соответствует структуре ваших облачных сегментов (см. раздел "Шаг 4. Настройка синхронизации с AWS и определение дальнейших действий" на стр. 806). (Однако зоны доступности и группы размещения не представлены в структуре AWS, подсети не представлены в структуре Microsoft Azure.) Пустые подгруппы внутри группы, обнаруженные при опросе, автоматически удаляются.

Вы также можете самостоятельно создавать группы администрирования, объединяющие все или некоторые устройства (см. раздел "Создание групп администрирования" на стр. 572).

Группа **Управляемые устройства\Cloud** по умолчанию наследует политики и задачи из группы **Управляемые устройства**. Вы можете изменить настройки параметров, если в свойствах параметров соответствующих политик и задач установлены флажки **Редактирование разрешено**.

Опрос облачного сегмента

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов облачных сегментов средствами AWS API или Azure API. На основании полученной информации Kaspersky Security Center обновляет состав и содержимое папок **Нераспределенные устройства** и **Управляемые устройства**. Если вы настроили автоматическое перемещение устройств в группы администрирования (см. раздел "Синхронизация с облачным окружением" на стр. 825), обнаруженные в сети устройства включаются в состав групп администрирования.

Чтобы Сервер администрирования мог опрашивать облачные сегменты, необходимы соответствующие права, которые обеспечивает IAM-роль (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 777) или учетная запись IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780) (в AWS), или идентификатор приложения и пароль (в Azure).

Вы можете добавлять и удалять соединения, а также настраивать для каждого облачного сегмента расписание опроса.

В этом разделе

Добавление соединений для опроса облачных сегментов

► *Чтобы добавить соединение для опроса облачных сегментов в список доступных, выполните следующие действия:*

1. В дереве консоли выберите узел **Обнаружение устройств** → **Cloud**.
2. В рабочей области окна нажмите **Настроить параметры опроса**.

   Откроется окно свойств со списком соединений, используемых для опроса облачных сегментов.
3. Нажмите на кнопку **Добавить**.

   Отобразится окно **Соединение**.
4. Настройте следующие параметры соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента.

   - **Облачное окружение**

     Облачное окружение, в котором расположены инстансы / виртуальные машины, может быть Amazon Web Services (AWS) или Microsoft Azure.

   Если вы выбрали AWS:

   - **Название соединения**

     Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

     Это имя будет также использоваться как имя группы администрирования для этих инстансов.

     Если вы планируете работать в двух облачных окружениях, AWS и Azure, вы можете захотеть назвать соединение "AWS Segment".

   - **Использовать AWS IAM-роль**

     Выберите этот вариант, если вы уже создали IAM-роль для работы Сервера администрирования с сервисами AWS (см. раздел "Создание IAM-роли для Сервера администрирования" на стр. 777).

   - **Использовать учетную запись AWS IAM-пользователя**

     Выберите этот вариант, если у вас есть учетная запись IAM-пользователя с необходимыми правами (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780) и вы можете ввести ID ключа и секретный ключ.

     - **ID ключа доступа**

       ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

- **Секретный ключ**

  Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя (см. раздел "Создание учетной записи IAM-пользователя для работы Kaspersky Security Center" на стр. 780).

  Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

  Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

Мастер настройки для работы в облачном окружении дает возможность указать только один ключ доступа AWS IAM. Впоследствии вы можете указывать и другие соединения для управления другими облачными сегментами (см. раздел "Добавление соединений для опроса облачных сегментов" на стр. 815).

Если вы выбрали Azure:

- **Название соединения**

  Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

  Это имя будет также использоваться как имя группы администрирования для этих инстансов.

  Если вы планируете работать в обоих облачных окружениях, AWS и Azure, вы можете захотеть назвать соединение "Azure Segment".

  В Kaspersky Security Center 11 можно опрашивать только один сегмент Azure. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

- **Пароль приложения в Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в

Azure (см. раздел "Создание подписки, идентификатора приложения и пароля" на стр. 791).

Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center (см. раздел "Создание учетной записи хранения Azure" на стр. 794).

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky Security Center.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

5. Если вы хотите, выберите **Настроить расписание опроса** и измените параметры заданные по умолчанию (см. раздел "Настройка расписания опроса" на стр. 819).

Соединение сохранится в параметрах программы.

После первого опроса нового облачного сегмента появится подгруппа в группе администрирования **Управляемые устройства\Cloud**, соответствующая этому сегменту.

Если вы указали неверные учетные данные, то инстансы не будут найдены во время опроса облачного сегмента, а новая подгруппа не будет отображаться в группе **Управляемые устройства\Cloud**.

Удаление соединений для опроса облачных сегментов

Если вам больше не нужно опрашивать какой-либо облачный сегмент, вы можете удалить соединение, соответствующее этому сегменту, из списка доступных. Вы также можете удалить соединение, если, например, права на опрос облачного сегмента перешли к другому AWS IAM-пользователю с другим ключом.

► *Чтобы удалить соединение, выполните следующие действия:*

1. В дереве консоли выберите узел **Обнаружение устройств** → **Cloud**.
2. В рабочей области окна выберите пункт **Настроить параметры опроса**.

   Появится окно со списком соединений, используемых для опроса облачных сегментов.
3. Выделите соединение, которое вы хотите удалить, и нажмите на кнопку **Удалить** в правой части окна.
4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Если вы удаляете соединение из списка доступных, то устройства, находящиеся внутри соответствующих сегментов, автоматически удалятся из соответствующих групп администрирования.

Настройка расписания опроса

Опрос облачного сегмента происходит по расписанию. Вы можете задать периодичность, с которой происходит опрос.

На этапе работы мастера настройки для работы в облачном окружении автоматически задается периодичность опроса раз в 5 минут. Вы можете изменить это значение в любое время и задать другое расписание. Не рекомендуется производить опрос чаще, чем раз в 5 минут, так как это может привести к ошибкам в работе AWS API или Azure API.

► *Чтобы настроить расписание опроса облачного сегмента, выполните следующие действия:*

1. В дереве консоли выберите узел **Обнаружение устройств** → **Cloud**.
2. В рабочей области нажмите **Настроить параметры опроса**.

   Откроется окно свойств объекта.
3. В списке выберите необходимое соединение нажмите на кнопку **Свойства**.

   Откроется окно свойств соединения.
4. В окне свойств перейдите по ссылке **Настроить расписание опроса**.

   Отобразится окно **Расписание**.
5. Настройте следующие параметры:
   - **Запуск по расписанию**

     Варианты расписания опроса:
     - **Каждый N день**

       Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

       По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.
     - **N минут**

       Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

       По умолчанию опрос запускается каждые 30 минут, начиная с текущего системного времени.
     - **По дням недели**

       Опрос выполняется регулярно, в указанные дни недели, в указанное время.

       По умолчанию опрос запускается каждую пятницу в 18:00:00.
     - **Ежемесячно, в указанные дни выбранных недель**

       Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное

время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Расписание опроса настроено и сохранено.

Установка программ на устройства в облачном окружении

Вы можете установить на устройства в облачном окружении следующие программы "Лаборатории Касперского": Kaspersky Security для Windows Server (для устройств с операционной системой Windows) и Kaspersky Endpoint Security для Linux (для устройств с операционной системой Linux).

Клиентские устройства, на которые вы планируете устанавливать защиту, должны соответствовать требованиям, установленным для работы Kaspersky Security Center в облачном окружении (см. раздел "Подготовка клиентских устройств в облачном окружении для работы с Kaspersky Security Center" на стр. 799). У вас должна быть действующая лицензия для установки программ на инстансы AWS и на виртуальные машины Microsoft Azure.

Kaspersky Security Center 11 поддерживает следующие сценарии:

- Клиентское устройство обнаружено с помощью AWS API; установка выполняется средствами AWS API.
- Клиентское устройство обнаружено с помощью опроса Active Directory, Windows-доменов или IP-диапазонов; установка выполняется средствами Kaspersky Security Center.

Другие способы установки программ не поддерживаются.

Для установки программ на виртуальные устройства используйте инсталляционные пакеты (см. раздел "Создание инсталляционных пакетов программ" на стр. 670).

► *Чтобы создать задачу удаленной установки программы на инстансы средствами AWS API или Azure API, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** выберите тип задачи **Удаленная установка программы**.
4. В окне **Выбор устройств** выберите нужные устройства из группы **Управляемые устройства\Cloud**.
5. Если на устройствах, на которые вы планируете установить программу, еще не установлен Агент администрирования, в окне **Выбор учетной записи для запуска задачи** выберите **Учетная запись требуется** и нажмите на кнопку **Добавить** в правой части окна. В появившемся меню выберите:

   - **Учетная запись в облачном окружении**

     Выберите этот параметр, если вы хотите установить программы на инстансы в среде AWS и получить ключ доступа AWS IAM с требуемыми правами, но не иметь IAM-роли. Также выберите этот параметр, если вы хотите установить программы на устройства в среде Azure.

     В появившемся окне предоставьте Kaspersky Security Center учетные данные, дающие право на установку программ на необходимые вам устройства (см. раздел "Шаг 3. Аутентификация в облачном окружении" на стр. 803).

Выберите облачное окружение AWS или Azure.

В поле **Имя учетной записи** введите имя для этих учетных данных. Вы увидите имя в списке учетных записей для запуска задачи.

Если вы выбрали AWS, в полях **ID ключа доступа** и **Секретный ключ** введите учетные данные IAM-пользователя, у которого есть права на установку программ на указанных устройствах.

Если вы выбрали Azure, в полях **Идентификатор подписки Azure** и **Пароль приложения в Azure** введите данные учетной записи Azure, у которой есть права на установку программ на указанных устройствах.

Если вы укажете неправильные учетные данные, задача удаленной установки программ закончится ошибкой на устройствах, для которых она запланирована.

- **Учетная запись**

  Для инстансов с операционной системой Windows выберите этот параметр, в случае если вы не будете устанавливать программу с использованием инструментов AWS или Azure API. В этом случае убедитесь, что устройства в вашем облачном сегменте соответствуют необходимым условиям (см. раздел "Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center" на стр. 117). Kaspersky Security Center выполнит установку программ собственными средствами без использования AWS или Azure API.

  Если вы укажете неправильные данные, задача удаленной установки программ закончится ошибкой на устройствах, для которых она запланирована.

- **IAM-роль**

  Выберите этот параметр, если вы хотите установить программы на инстансы в окружении AWS и иметь IAM-роль с требуемыми правами (см. раздел "Создание IAM-роли для установки программ на инстансы Amazon EC2" на стр. 781).

  Если вы выберете этот параметр, у вас не будет IAM-роли с требуемыми правами и задача удаленной установки программ завершится с ошибкой на устройствах, для которых она запланирована.

- **SSH сертификат**

  Для инстансов с операционной системой Linux выберите этот параметр в случае, если вы не будете устанавливать программу с использованием инструментов AWS API или Azure API. В этом случае убедитесь, что устройства в вашем облачном сегменте соответствуют необходимым условиям (см. раздел "Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center" на стр. 117). Kaspersky Security Center выполнит установку программ собственными средствами без использования AWS или Azure API.

Вы можете предоставить несколько учетных данных, каждый раз нажимая на кнопку **Добавить**. Если разные облачные сегменты требуют разных учетных данных, укажите учетные данные для всех сегментов.

Задача удаленной установки программы появится в списке задач в рабочей области папки **Задачи**.

В Microsoft Azure удаленная установка программ безопасности на виртуальную машину может быть результатом удаления расширения Custom Scrip, установленного на этой виртуальной машине.

Просмотр свойств облачных устройств

► *Чтобы просмотреть свойства инстанса, выполните следующие действия:*

1. В дереве консоли в папке **Обнаружение устройств** → **Cloud** выберите папку, соответствующую той группе, в которой находится интересующий вас инстанс.

   Если вы не знаете, в какой группе находится нужное вам виртуальное устройство, воспользуйтесь поиском:

   a. Правой клавишей мыши нажмите на название узла **Управляемые устройства** → **Cloud** и в контекстном меню выберите **Поиск**.

   b. В появившемся окне выполните поиск (см. раздел "Параметры поиска устройств" на стр. 867).

      Если устройство, соответствующее введенным критериям, существует, то его имя и информация о нем будут отображены в нижней части окна.

2. Нажмите на название нужного узла правой клавишей мыши. В контекстном меню выберите пункт **Свойства**.

   В появившемся окне отобразятся свойства объекта.

3. В разделе **Информация о системе** → Общая информация о системе содержатся параметры, которые специфичны для устройств в облачном окружении:

   - Устройство обнаружено с помощью API

     Для инстансов EC2, обнаруженных средствами AWS API, отображается значение параметра **AWS**. Для виртуальных машин Azure обнаруженных с использованием инструментов Azure API, отображается значение **Azure**. Если устройство не может быть обнаружено средствами API, то отображается значение **Нет**.

   - Регион облачного окружения.
   - VPC (только для инстансов Amazon EC2, обнаруженных с использованием AWS API).
   - Облачная зона доступности (только для инстансов Amazon EC2, обнаруженных с использованием AWS API).
   - Облачная подсеть (отсутствует для виртуальных машин Azure Classic).
   - Облачная группа размещения (только для инстансов Amazon EC2 обнаруженных с использованием AWS API; это устройство не отображается, если инстанс не принадлежит группе размещения).

Чтобы экспортировать эту информацию в файл формата CSV или TXT, нажмите на кнопку **Экспортировать в файл**.

Синхронизация с облачным окружением

Во время работы мастера настройки для работы в облачном окружении автоматически создается правило Синхронизация с облачным окружением. Правило позволяет автоматически перемещать инстансы, найденные при каждом опросе, из группы **Нераспределенные устройства** в группу **Управляемые устройства\Cloud**, чтобы инстансы были доступны для централизованного управления. По умолчанию правило включено после создания. Вы можете выключить, изменить или форсировать правило в любое время.

► *Чтобы изменить свойства правила Синхронизация с облачным окружением и / или форсировать правило, выполните следующие действия:*

1. Нажмите правой клавишей мыши на название узла **Обнаружение устройств** в дереве консоли.
2. В контекстном меню выберите пункт **Свойства**.
3. В открывшемся окне свойств выберите раздел **Перемещение устройств**.
4. В списке правил перемещения устройств выберите **Синхронизация с облачным окружением** и нажмите на кнопку **Свойства** внизу окна.

   Откроется окно свойств правила.
5. При необходимости укажите следующие параметры в блоке параметров **Облачные сегменты**:

   - **Устройство находится в облачном сегменте**

     Правило применяется только на устройствах, которые находятся в выбранном облачном сегменте. В противном случае правило применяется на всех обнаруженных устройствах.

     По умолчанию выбран этот вариант.

   - **Включать дочерние объекты**

     Правило выполняется для всех устройств в выбранном сегменте и во всех его вложенных облачных разделах. В противном случае правило будет действовать для устройств, которые находятся в корневом сегменте.

     По умолчанию выбран этот вариант.

   - **Перемещать устройства из вложенных объектов в соответствующие подгруппы**

     Если параметр включен, то устройства из вложенных объектов перемещаются в подгруппы, соответствующие их структуре.

     Если параметр выключен, то устройства из вложенных объектов перемещаются в корень подгруппы Cloud без разбиения на подгруппы.

     По умолчанию параметр включен.

   - **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**

     Если флажок установлен, то если в структуре групп **Управляемые устройства\Cloud**

нет подгруппы, соответствующей тому разделу, в котором находится устройство, Kaspersky Security Center создаст такую подгруппу. Например, если в процессе обнаружения устройств была найдена новая подсеть, то в группе **Управляемые устройства\Cloud** будет создана новая группа с таким же именем.

Если параметр выключен, Kaspersky Security Center не создает подгруппы. Например, если новая подсеть была обнаружена во время опроса сети, то новая группа с таким же именем не будет создана под группой **Управляемые устройства\Cloud**, и устройства, которые находятся в этой подсети, не будут перемещены в группу **Управляемые устройства\Cloud**.

По умолчанию параметр включен.

- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**

  Если параметр включен, то программа удалит из группы Cloud подгруппы, не соответствующие никаким облачным объектам.

  Если параметр выключен, то подгруппы, не соответствующие облачным объектам, будут сохраняться.

  По умолчанию параметр включен.

Если на этапе прохождения мастера настройки для работы в облачном окружении вы устанавливали флажок **Синхронизация с облачным окружением**, то правило Синхронизация с облачным окружением создается с установленными флажками **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах**.

Если вы не включили параметр **Синхронизация с облачным окружением**, правило будет создано с выключенным параметром. Если в процессе работы с Kaspersky Security Center вам потребуется, чтобы структура подгрупп внутри подгруппы **Управляемые устройства\Cloud** соответствовала структуре облачных сегментов, включите в свойствах правила параметры **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах** и форсируйте правило.

6. Выберите значение в раскрывающемся списке **Устройство обнаружено с помощью API**:

   - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.
   - **Azure** Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.
   - **Нет**. Устройство не обнаруживается с помощью AWS API или Azure API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью API.
   - Не задано. Критерий не применяется.

7. При необходимости настройте другие свойства правила в других разделах (см. раздел "Параметры поиска устройств" на стр. 867).

8. При необходимости форсируйте правило, нажав на кнопку **Форсировать** внизу окна.

   Будет запущен мастер выполнения правила. Следуйте далее указаниям мастера. После окончания работы мастера правило будет запущено и структура групп внутри подгруппы **Управляемые устройства\Cloud** будет соответствовать структуре ваших облачных сегментов.

9. Нажмите на кнопку **ОК**.

Параметры настроены и сохранены.

► *Чтобы выключить правило Синхронизация с Cloud, выполните следующие действия:*

1. Нажмите правой клавишей мыши на название узла **Обнаружение устройств** в дереве консоли.
2. В контекстном меню выберите пункт **Свойства**.
3. В открывшемся окне свойств выберите раздел **Перемещение устройств**.
4. В списке правил перемещения устройств выключите параметр **Синхронизация с облачным окружением** и нажмите на кнопку **ОК**.

Правило выключено и больше не применяется.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов "Лаборатории Касперского" Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, программы еще раз проведут контроль целостности загружаемых обновлений.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений программы на дисках.

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 (https://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/subscribehttp://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо 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 (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского".

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. 939).

Устранение неисправностей

В этом разделе содержится информация о наиболее распространенных ошибках и проблемах при развертывании и использовании Kaspersky Security Center, а также рекомендации по решению проблем.

В этом разделе

Проблемы при удаленной установке программ

В таблице ниже перечислены проблемы, возникающие при удаленной установке программ, и типовые причины возникновения этих проблем.

Таблица 65. Проблемы при удаленной установке программ

Проблема	Типовая причина проблемы и вариант решения
Недостаточно прав для установки	Учетная запись, под которой запущена установка, не имеет достаточно прав для выполнения операций, необходимых для установки программы.
Недостаточно места на диске	Недостаточно свободного места на диске для завершения установки. Освободите место на диске и повторите операцию.
Произошла незапланированная перезагрузка ОС	Во время установки произошла незапланированная перезагрузка ОС, точный результат установки может быть неизвестен. Проверьте правильность параметров запуска инсталляционного приложения или обратитесь в Службу технической поддержки.
Не найден необходимый файл	В инсталляционном пакете не найден необходимый файл. Проверьте целостность используемого инсталляционного пакета.
Несовместимая платформа	Инсталляционный пакет не предназначен для данной платформы. Используйте соответствующий инсталляционный пакет.
Несовместимая программа	На устройстве установлена программа, несовместимая с устанавливаемой программой. Перед установкой удалите все программы, входящие в список несовместимых.

Проблема	Типовая причина проблемы и вариант решения
Недостаточные системные требования	Инсталляционный пакет требует наличия в системе дополнительного программного обеспечения. Проверьте соответствие конфигурации системы системным требованиям устанавливаемой программы.
Незавершенная установка	Предыдущая установка или удаление программы не было штатно завершено. Для завершения предыдущей установки или удаления программы, выполненного на данном устройстве, необходимо перезагрузить ОС и повторить процесс установки.
Не та версия инсталляционного приложения	Установка данного инсталляционного пакета не поддерживается версией инсталляционного приложения, установленного на устройстве.
Инсталляция уже запущена	На устройстве уже запущена установка другого приложения.
Не удалось открыть инсталляционный пакет	Возможные причины: пакет отсутствует, пакет поврежден, недостаточно прав для доступа к пакету.
Несовместимая локализация	Инсталляционный пакет не предназначен для установки на данную локализацию ОС.
Установка запрещена политикой	Установка программ на данном устройстве запрещена политикой.
Ошибка записи файла	Во время установки программы произошла ошибка записи. Проверьте наличие прав у учетной записи, под которой выполняется установка, и наличие свободного места на диске.
Неверный пароль деинсталляции	Пароль для удаления программы задан неверно.
Недостаточные аппаратные требования	Аппаратные требования системы не удовлетворяют требованиям программы (объем оперативной памяти, свободное место на диске и так далее).
Недопустимый каталог установки	Установка программы в указанный каталог запрещена политикой инсталляционного приложения.
Требуется повторная попытка установки после перезагрузки устройства	Требуется повторный запуск инсталлятора программы после перезагрузки устройства.
Для продолжения установки требуется перезагрузка устройства	Для продолжения работы инсталлятора программы требуется перезагрузка устройства.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания (см. раздел "Развертывание захватом и копированием образа жесткого

диска устройства" на стр. 113), часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом "-dupfix".

  На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

  Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

  > Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

  Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

  На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

  - Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

    ```
    REGEDIT4

    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

    "KLSRV_CheckClones"=dword:00000003
    ```

  - Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\Se
"KLSRV_CheckClones"=dword:00000003
```

Проверка участия Агента администрирования в Kaspersky Security Network

Если управляемое устройство с операционной системой Windows покидает сеть (например, пользователь выкупает устройство у компании и использует его как собственное устройство), Агент администрирования на этом устройстве может продолжать участвовать в Kaspersky Security Network. Например, это может произойти, если устройству была назначена точка распространения.

► *Чтобы проверить, участвует ли Агент администрирования в Kaspersky Security Network, выполните следующие действия:*

1. В Windows откройте окно **Службы** (**Панель управления** → **Администрирование** → **Службы**).
2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network.

При необходимости службу ksnproxy можно выключить. При этом Агент администрирования на вашем устройстве перестанет участвовать в Kaspersky Security Network. Для этого требуются права локального администратора.

Проблемы с Сервером мобильных устройств Exchange ActiveSync

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера мобильных устройств Exchange ActiveSync.

Ошибка во время установки Сервера мобильных устройств Exchange ActiveSync

Если во время локальной или удаленной установки возникла ошибка, то причину ошибки можно узнать, открыв файл error.log, который расположен на устройстве, где производилась установка программы, по пути C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (где цифры – это дата и время установки программы). Как правило, информации из файла error.log достаточно для решения возникшей проблемы.

В таблице ниже приведены примеры типичных ошибок, регистрируемых в файле error.log.

Таблица 66. Типичные ошибки

Ошибка	Описание	Причина

Ошибка	Описание	Причина
На шаге установки "Проверка подключения к PowerShell" произошла ошибка	Ошибка: "Сбой при обработке данных, полученных от удаленного сервера". Сообщение об ошибке: "Пользователю oreh-security.ru/Users/TestInstall не назначена ни одна из ролей управления".	Учетная запись, под которой производилась установка программы, не обладает ролью Organization Management.
На шаге установки "Проверка подключения к PowerShell" произошла ошибка	Не удалось подключиться к удаленному серверу. Сообщение об ошибке: "Клиент WinRM не может обработать запрос". Сервер не поддерживает механизм аутентификации, запрашиваемый клиентом, или в параметрах службы отключен незашифрованный трафик. Проверьте, включен ли незашифрованный трафик в параметрах службы или укажите один из поддерживаемых сервером механизмов аутентификации. Для использования аутентификации Kerberos укажите имя компьютера как удаленную папку. Также проверьте, что клиентский компьютер и компьютер назначения находятся в одном домене. Для использования базовой аутентификации укажите имя компьютера как удаленную папку, выберите базовую аутентификацию и укажите имя пользователя и пароль. Возможный механизм аутентификации по данным сервера: Digest. Дополнительную информацию см. в разделе справки about_Remote_Troubleshooting.	Механизм аутентификации Windows в настройках веб-сервера IIS для виртуальной директории PowerShell не включен.

Список устройств и почтовых аккаунтов пуст

Причину, из-за которой не удается получить список устройств и почтовых аккаунтов, можно узнать из событий, сохраненных в Консоли администрирования в узле Сервер администрирования на закладке **События** в выборке событий **Отказы функционирования**. Если в событиях нет информации, необходимо проверить подключение между Агентом администрирования устройства, на котором развернут Сервер

мобильных устройств Exchange ActiveSync и Сервером администрирования.

Проблемы с Сервером iOS MDM

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера iOS MDM, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru

Информация о некоторых проблемах, возникающих при использовании Сервера iOS MDM, приведена в Базе знаний на веб-сайте Службы технической поддержкиhttp://support.kaspersky.com/ks10mob.

Проверка доступности сервиса APN

Для проверки доступности сервиса APN вы можете использовать следующие команды утилиты Telnet:

- Со стороны веб-сервиса iOS MDM:

```
$ telnet gateway.push.apple.com 2195
```

- Со стороны iOS MDM-устройства (проверку необходимо провести из сети, в которой находится устройство):

```
$ telnet 1-courier.push.apple.com 5223
```

Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM

► *Если при использовании веб-сервиса iOS MDM возникают проблемы, выполните следующие действия:*

1. Проверьте, что сертификаты корректны.
2. Проверьте события Консоли администрирования на наличие ошибок и невыполненных команд со стороны Сервера iOS MDM.

3. Проверьте мобильное устройство с помощью консоли приложения iPhone Configuration Utility.
4. Проверьте файлы трассировки веб-сервиса iOS MDM: внутренние сервисы, такие как RPC-сервис и веб-сервис (100 потоков), должны быть успешно запущены.

Проверка корректности сертификата веб-сервиса iOS MDM с помощью мультиплатформенной утилиты OpenSSL

Пример команды:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

Результат выполнения:

```
CONNECTED(00000003)
...
---
Цепочка сертификатов
0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com
i:/CN=Kaspersky iOS MDM Server CA
...
.
```

Проверка трассировок веб-сервиса iOS MDM

О том, как получить трассировки веб-сервиса iOS MDM, см. статью в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/9792.

Пример успешных трассировок:

```
I1117 20:58:39.050226    7984] [MAIN]: Starting service...
I1117 20:58:39.050226    7984] [RPC]: Starting rpc service...
...
I1117 20:58:39.081428    7984] [RPC]: Rpc service started
I1117 20:58:39.081428    3724] [WEB]: Starting web service...
I1117 20:58:39.455832    3724] [WEB]: Starting thread [T000]
I1117 20:58:39.455832    3724] [WEB]: Starting thread [T001]
...
I1117 20:58:39.455832    3724] [WEB]: Starting thread [T099]
```

Пример трассировок с занятым портом:

[WEB]: Starting web service...

Error 28 fault: SOAP-ENV:Server [no subcode] "Only one usage of each socket address (protocol/network address/port) is no

Detail: [no detail]

[WEB]: Web service terminated

Проверка трассировок с помощью консоли приложения iPhone Configuration Utility

Пример успешных трассировок:

Службы, отвечающие за MDM – profiled, mdmd

mdmd[174] <Notice>: (Note) MDM: mdmd starting...

mdmd[174] <Notice>: (Note) MDM: Looking for managed app states to clean up

profiled[175] <Notice>: (Note) profiled: Service starting...

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Polling MDM server https://10.255.136.71 for commands

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Состояние: 200

mdmd[174] <Notice>: (Note) MDM: Attempting to perform MDM request: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Handling request type: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Command Status: Acknowledged

profiled[175] <Notice>: (Note) profiled: Recomputing passcode requirement message

profiled[175] <Notice>: (Note) profiled: Locking device

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Состояние: 200

mdmd[174] <Notice>: (Note) MDM: Server has no commands for this device.

mdmd[174] <Notice>: (Note) MDM: mdmd stopping...

Проблемы с KES-устройствами

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием KES-устройств, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru

Информация о проблемах, возникающих при работе с KES-устройствами, приведена в Базе знаний на веб-сайте Службы технической поддержки http://support.kaspersky.com/ks10mob.

Проверка настроек сервиса Google Firebase Cloud Messaging

Проверка настроек сервиса Google Firebase Cloud Messaging может быть выполнена на портале Google https://code.google.com/apis/console/#project:[YOUR PROJECT NUMBER]:access.

Проверка доступности сервиса Google Firebase Cloud Messaging

Для проверки доступности сервиса Google Firebase Cloud Messaging со стороны Kaspersky Security Center (см. раздел "Использование Google Firebase Cloud Messaging" на стр. 173), вы можете использовать команду утилиты Telnet:

```
telnet android.googleapis.com 443
```

Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center.

В этом разделе

Характеристики и ограничения Kaspersky Security Center

В этом разделе содержится информация о характеристиках и ограничениях Kaspersky Security Center.

В этом разделе

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в

перечне аппаратных и программных требований (на стр. 23).

Сервер администрирования и SQL-сервер на разных устройствах, в сети 50 000 устройств

Таблица 67. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядер, 2500 МГц
ОЗУ	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит

Таблица 68. Конфигурация устройства с SQL-сервером

Оборудование	Значение
Процессор	4 ядер, 2500 МГц
ОЗУ	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 50 000 устройств

Таблица 69. Конфигурация устройства с Сервером администрирования и SQL-сервером

Оборудование	Значение
Процессор	8 ядер, 2500 МГц
ОЗУ	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 100 000 устройств

Таблица 70. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер, 2,13 ГГц
ОЗУ	8 ГБ
Жесткий диск	1 ТБ, RAID
Сетевой адаптер	1 Гбит

Таблица 71. Конфигурация устройства с SQL Server

Оборудование	Значение
Процессор	8 ядер, 2,53 ГГц
ОЗУ	26 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение точек распространения, либо точки распространения назначены вручную по рекомендуемой таблице (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 88);
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 561);
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 72. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Требования для точки распространения

Чтобы обрабатывать до 10 000 клиентских устройств, точка распространения должна отвечать следующим требованиям (предоставлена конфигурация тестового стенда):

- Процессор: Intel® Core™ i7-7700 CPU, 3.60ГГц, 4 ядра.
- ОЗУ: 8 ГБ.
- Диск: Intel SSDSC2KW120H6.

Кроме того, точка распространения должна иметь доступ в интернет и должна быть всегда включена.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с точкой

распространения дополнительно потребуется дисковое пространство, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Предварительный расчет места в базе данных и на диске для Сервера администрирования

Оценка места в базе данных Сервера администрирования

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(200 * C + 2.3 * E + 2.5 * A), КБ,

где:

"C" – количество устройств.

"E" – количество сохраняемых событий.

"A" – суммарное количество объектов Active Directory:

- учетных записей устройств;
- учетные записи пользователей;
- учетных записей групп безопасности;
- подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Если Сервер администрирования распространяет обновления Windows (играет роль WSUS-сервера), то в базе данных дополнительно потребуется 2,5 ГБ.

Следует учитывать, что в ходе работы в базе данных всегда образуется так называемое "незанятое пространство" (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД "SQL Server") часто оказывается примерно в два раза больше, чем занятое в базе данных место.

Размер журнала транзакций (по умолчанию файл KAV_log.LDF в случае использования СУБД "SQL Server") может достигать 2 ГБ.

Оценка места на диске для устройства с Сервером администрирования

Место на диске в директории %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit на устройстве с Сервером администрирования можно приблизительно оценить по формуле:

(220 * C + 0.15 * E + 0.17 * A), КБ

Значения переменных "C", "E" и "A" см. выше.

Расчет дополнительного места на диске с учетом использования Системного администрирования:

- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.
- Патчи. Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:
  - Папка для хранения патчей должна иметь объем дискового пространства, равный суммарному размеру всех загруженных патчей. По умолчанию патчи хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (вы можете назначить для хранения патчей другую папку при помощи утилиты klsrvswch). Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.
  - В папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру тех патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Оценка трафика между Агентом администрирования и Сервером администрирования

В таблице ниже приведен среднесуточный трафик между Сервером администрирования Kaspersky Security Center 11 и управляемым устройством, на котором установлены Агент администрирования и Kaspersky Endpoint Security 11 для Windows.

Таблица 73. Среднесуточный трафик: Kaspersky Security Center 11

	От Сервера к управляемому устройству (download)	От управляемого устройства к Серверу (upload)
Средний ежесуточный трафик с параметрами задачи обновления по умолчанию	52 МБ	4 МБ
Средний ежесуточный трафик с выключенной задачей обновления	836 КБ	726 КБ

Дополнительные возможности

В этом разделе рассматривается ряд дополнительных функций программы Kaspersky Security Center, предназначенных для расширения возможностей централизованного управления программами на устройствах.

В этом разделе

Автоматизация работы Kaspersky Security Center. Утилита klakaut

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center.

Работа с внешними инструментами

Kaspersky Security Center позволяет сформировать список *внешних инструментов* (далее также *инструментов*) – программ, которые вызываются для клиентского устройства из Консоли администрирования при помощи группы контекстного меню **Внешние инструменты**. Для каждого инструмента из списка создается отдельная команда меню, с помощью которой Консоль администрирования запускает соответствующую инструменту программу.

Программа запускается на рабочем месте администратора. В качестве аргументов командной строки программа может принимать атрибуты удаленного клиентского устройства (NetBIOS-имя, DNS-имя, IP-адрес). Подключение к удаленному устройству может выполняться при помощи туннелированного соединения.

По умолчанию для каждого клиентского устройства список внешних инструментов содержит следующие

сервисные программы:

- **Удаленная диагностика** – утилита удаленной диагностики Kaspersky Security Center.
- **Удаленный рабочий стол** – стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу".
- **Управление компьютером** – стандартный компонент Microsoft Windows.

► *Чтобы добавить или удалить внешние инструменты, а также изменить их параметры,*

в контекстном меню клиентского устройства выберите пункт **Внешние инструменты** → **Настроить внешние инструменты**.

В результате откроется окно **Внешние инструменты**. В этом окне вы можете добавлять и удалять внешние инструменты, а также настраивать их параметры с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Консоли администрирования одним значком. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со значком в Консоли администрирования.

Избежать проблемы с неверным отображением новых устройств в Консоли администрирования после клонирования помогает специальный *режим клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одним значком в Консоли администрирования. По завершении клонирования образа "эталонного" устройства, новые устройства отображаются в Консоли администрирования нормально (отдельными значками).

Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты klnagchk (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk" на стр. 593).
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое

количество перезагрузок устройства.

5. Администратор выполняет клонирование жесткого диска "эталонного" устройства на любое число устройств.
6. Для каждой клонированной копии должны быть выполнены следующие условия:
   a. имя устройства изменено;
   b. устройство перезагружено;
   c. режим клонирования диска выключен.

Включение и выключение режима клонирования диска с помощью утилиты klmover

► *Чтобы включить / выключить режим клонирования диска Агента администрирования, выполните следующие действия:*

1. Запустите утилиту klmover на устройстве с установленным Агентом администрирования, который нужно клонировать.

   Утилита klmover находится в папке установки Агента администрирования.
2. Чтобы включить режим клонирования диска, в командной строке Windows введите команду `klmover -cloningmode 1`.

   Агент администрирования переключается в режим клонирования диска.
3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду `klmover -cloningmode`.

   В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.
4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду `klmover -cloningmode 0`.

Настройка получения сообщений от компонента Контроль целостности системы

Управляемые программы, такие как Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент, отправляют сообщения от компоненты Контроль целостности системы в Kaspersky Security Center. Kaspersky Security Center позволяет также следить за неизменностью критически важных областей систем (например, веб-серверы, банкоматы) и оперативно реагировать на нарушения целостности таких систем. Для этого реализована поддержка получения сообщений от компонента Контроль целостности системы. Компонент Контроль целостности системы позволяет следить не только за файловой системой устройства, но и за ветками реестра, состоянием сетевого экрана и состоянием подключенного оборудования.

Требуется выполнить настройку Kaspersky Security Center, чтобы получать сообщения от компонента Контроль целостности системы без использования программ Kaspersky Security для Windows Server или

Kaspersky Security для виртуальных сред Легкий агент.

► *Чтобы настроить параметры получения сообщений от компонента Контроль целостности системы, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags
3. Создайте ключи:
   - Создайте ключ KLSRV_EVP_FIM_PERIOD_SEC, чтобы указать интервал времени подсчета числа обработанных событий. Задайте следующие параметры:
     a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_SEC.
     b. Укажите тип ключа DWORD.
     c. Задайте диапазон значений промежутка времени от 43 200 до 172 800 секунд. По умолчанию промежуток проверки равен 86 400 секунд.
   - Создайте ключ KLSRV_EVP_FIM_LIMIT для ограничения количества принимаемых событий за указанный промежуток времени. Задайте следующие параметры:
     a. Укажите название ключа KLSRV_EVP_FIM_LIMIT.
     b. Укажите тип ключа DWORD.
     c. Задайте диапазон значений принимаемых событий от 2000 до 50 000. По умолчанию количество событий равно 2000.
   - Создайте ключ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC для подсчета событий с точностью до определенного промежутка времени. Задайте следующие параметры:
     a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.
     b. Укажите тип ключа DWORD.
     c. Задайте диапазон значений от 120 до 600 секунд. Временной интервал, установленный по умолчанию, составляет 300 секунд.
   - Создайте ключ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, чтобы после указанного значения времени программа выполняла проверку того, что число событий, обработанных за промежуток времени, становится меньше заданного ограничения. Проверка выполняется при достижении ограничения приема событий. Если условие выполняется, возобновляется сохранение событий в базу данных. Задайте следующие параметры:

a. Укажите название ключа KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

b. Укажите тип ключа DWORD.

c. Задайте диапазон значений от 600 до 3 600 секунд. Временной интервал, установленный по умолчанию, составляет 1 800 секунд.

Если ключи не созданы, используются значения по умолчанию.

4. Перезапустите службу Сервера администрирования.

Ограничения получения событий от компонента Контроля целостности системы будут настроены. Результаты работы компоненты Контроля целостности системы вы можете посмотреть в отчетах **10 правил Контроля целостности системы, которые чаще всего срабатывали на устройствах,** и **10 устройств, на которых произошло максимальное количество срабатываний правил Контроля целостности системы**.

Обслуживание базы данных Сервера администрирования

Обслуживание базы данных Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать базу данных Сервера администрирования не реже раза в неделю.

Обслуживание базы данных Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания базы данных программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (если необходимо).

Задача обслуживания базы данных Сервера администрирования не поддерживает MySQL. Если в качестве СУБД используется MySQL, администратору следует обслуживать базу данных самостоятельно.

► *Чтобы создать задачу обслуживания базы данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел Сервера администрирования, для которого нужно создать задачу обслуживания базы данных.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи.
4. В окне мастера **Выбор типа задачи** выберите тип задачи **Обслуживание баз данных** и нажмите на кнопку **Далее**.

5. Если во время обслуживания нужно сжимать базу данных Сервера администрирования, в окне мастера **Параметры** установите флажок **Сжать базу данных**.
6. Следуйте дальнейшим шагам мастера.

Созданная задача отображается в списке задач в рабочей области папки **Задачи**. Для одного Сервера администрирования может выполняться только одна задача обслуживания баз. Если задача обслуживания баз для Сервера администрирования уже создана, создание еще одной задачи обслуживания баз невозможно.

Окно Способ уведомления пользователей

В окне **Способ уведомления пользователя** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство:

- **Показать ссылку в мастере**. При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.
- **Отправить ссылку пользователю**. При выборе этого варианта вы можете настроить параметры оповещения пользователя о подключении устройства.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер (см. раздел "Шаг 6. Настройка параметров отправки почтовых уведомлений" на стр. 218).

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

По ссылке **Изменить сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

См. также:

Установка сертификата пользователю.....653

Раздел Общие

В этом разделе можно настраивать общие параметры профиля для мобильных устройств Exchange ActiveSync.

Имя.

Название профиля.

Разрешить неинициализируемые устройства

Если флажок установлен, устройствам, которым доступны не все параметры

политики Exchange ActiveSync, разрешено подключение к Серверу мобильных устройств.

Если флажок снят, подключение таких устройств к Серверу мобильных устройств запрещено.

По умолчанию флажок установлен.

Период обновления (ч)

Если флажок установлен, программа обновляет информацию о политике Exchange ActiveSync с интервалом, указанным в поле ввода.

Если флажок снят, информация о политике Exchange ActiveSync не обновляется.

По умолчанию флажок установлен, интервал обновления составляет один час.

Окно Выборка устройств

В этом окне можно указать выборку устройств, сведения о которых будут отображаться в рабочей области на закладке **Статистика** узла **Отчеты и уведомления**.

Выберите выборку из списка **Выборка устройств**. В списке перечислены выборки, заданные по умолчанию, и выборки, созданные пользователем.

Окно Определение названия создаваемого объекта

В окне укажите название создаваемого объекта. Имя не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

Раздел Категории программ

В этом разделе можно настроить распространение информации о категориях программ на клиентские устройства.

Передавать все данные (для Агентов администрирования версии Service Pack 2 и ниже)

Если выбран этот вариант, при изменении категории программ на клиентские устройства передаются все данные категории. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и ниже.

Передавать только измененные данные (для Агентов администрирования версии Service Pack 2 и выше)

Если выбран этот вариант, при изменении категории программ на клиентские устройства передаются не все данные категории, а только те данные, которые были изменены. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и выше.

См. также:

Особенности работы с интерфейсом управления

Этот раздел содержит описание приемов работы в главном окне Kaspersky Security Center.

В этом разделе

Как вернуть исчезнувшее окно свойств

Иногда открытое окно свойств объекта исчезает с экрана. Это происходит из-за того, что оно перекрывается главным окном программы (эта ситуация является особенностью работы Microsoft Management Console).

► *Чтобы перейти к исчезнувшему окну свойств объекта,*

нажмите комбинацию клавиш **ALT+TAB**.

Как обновить данные в рабочей области

В Kaspersky Security Center данные рабочей области (такие как статусы устройств, статистика и отчеты) никогда не обновляются автоматически.

► *Чтобы обновить данные в рабочей области, выполните одно из следующих действий:*

- нажмите на клавишу **F5**;
- в контекстном меню объекта в дереве консоли выберите пункт **Обновить**;

- нажмите на кнопку  , расположенную в рабочей области.

Как перемещаться по дереву консоли

Для перемещения по дереву консоли вы можете использовать следующие кнопки, расположенные в панели инструментов:

-  – переход на один шаг назад;
-  – переход на один шаг вперед;
-  – переход на один уровень вверх.

Можно также воспользоваться навигационной цепочкой, расположенной в правом верхнем углу рабочей области. Навигационная цепочка содержит полный путь к той папке дерева консоли, в которой вы находитесь в текущий момент. Все элементы цепочки, кроме последнего, являются ссылками на объекты дерева консоли.

Как открыть окно свойств объекта в рабочей области

Свойства большинства объектов Консоли администрирования можно изменять в окне свойств объекта.

► *Чтобы открыть окно свойств объекта, расположенного в рабочей области, выполните одно из следующих действий:*

- в контекстном меню объекта выберите пункт **Свойства**;
- выберите объект и нажмите комбинацию клавиш **ALT**+**ENTER**.

Как выбрать группу объектов в рабочей области

Вы можете выбрать группу объектов в рабочей области. Выбор группы объектов можно использовать, например, для создания набора устройств и последующего формирования задач для него.

► *Чтобы выбрать диапазон объектов, выполните следующие действия:*

1. Выберите первый объект диапазона и нажмите на клавишу **SHIFT**.
2. Удерживая нажатой клавишу **SHIFT**, выберите последний объект диапазона.

Диапазон будет выбран.

► *Чтобы объединить отдельные объекты в группу, выполните следующие действия:*

1. Выберите первый объект в составе группы и нажмите на клавишу **CTRL**.
2. Удерживая нажатой клавишу **CTRL**, выберите остальные объекты группы.

Объекты будут объединены в группу.

Как изменить набор граф в рабочей области

Консоль администрирования позволяет изменять набор граф, отображаемых в рабочей области.

► *Чтобы изменить набор граф в рабочей области, выполните следующие действия:*

1. Выберите объект дерева консоли, для которого вы хотите изменить набор граф.
2. В рабочей области папки откройте окно настройки набора граф по ссылке **Добавить или удалить графы**.
3. В окне **Добавление или удаление граф** сформируйте набор граф для отображения.

Справочная информация

В этом разделе в таблицах представлена сводная информация о контекстном меню объектов Консоли администрирования, а также о статусах объектов дерева консоли и рабочей области.

В этом разделе

Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

Таблица 74. Элементы контекстного меню объектов Консоли администрирования

Объект	Пункт меню	Назначение пункта меню
Общие пункты контекстного меню	**Поиск**	Открыть окно поиска устройств.
	Обновить	Обновить отображение выбранного объекта.
	Экспортировать список	Экспортировать текущий список в файл.

Объект	Пункт меню	Назначение пункта меню
	Свойства	Открыть окно свойств выбранного объекта.
	Вид → Добавить или удалить графы	Добавить или удалить графы в таблице объектов в рабочей области.
	Вид → Крупные значки	Отображать объекты в рабочей области в виде крупных значков.
	Вид → Мелкие значки	Отображать объекты в рабочей области в виде мелких значков.
	Вид → Список	Отображать объекты в рабочей области в виде списка.
	Вид → Таблица	Отображать объекты в рабочей области в виде таблицы.
	Вид → Настроить	Настроить отображение элементов Консоли управления.
Kaspersky Security Center	**Создать → Сервер администрирования**	Добавить в дерево консоли Сервер администрирования.
Параметры Сервера администрирования	**Подключиться к Серверу администрирования**	Подключиться к Серверу администрирования.
	Отключиться от Сервера администрирования	Отключиться от Сервера администрирования.
Управляемые устройства	**Установить программу**	Запустить мастер удаленной установки программы.
	Вид → Настройка интерфейса	Настроить отображение элементов интерфейса.
	Удалить	Удалить Сервер администрирования из дерева консоли.
	Установить программу	Запустить мастер удаленной установки для группы администрирования.

Объект	Пункт меню	Назначение пункта меню
	Обнулить счетчик вирусов	Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования.
	Просмотреть отчет об угрозах	Создать отчет об угрозах и вирусной активности устройств, входящих в состав группы администрирования.
	Создать → Группу	Создать группу администрирования.
	Все задачи → Новая структура групп	Создать структуру групп администрирования на основе структуры доменов или Active Directory.
	Все задачи → Показать сообщение	Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования.
Управляемые устройства → Серверы администрирования	**Создать → Подчиненный Сервер администрирования**	Запустить мастер добавления подчиненного Сервера администрирования.
	Создать → Виртуальный Сервер администрирования	Запустить мастер добавления виртуального Сервера администрирования.
Управление мобильными устройствами → Мобильные устройства	**Создать → Мобильное устройство**	Подключить новое мобильное устройство пользователя.
Управление мобильными устройствами → Сертификаты	**Создать → Сертификат**	Создать сертификат.
	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Выборки устройств	**Создать → Новая выборка**	Создать выборку устройств.
	Все задачи → Импортировать	Импортировать выборку из файла.
Лицензии Лаборатории Касперского	**Добавить код активации или ключ**	Добавить ключ в хранилище Сервера администрирования.

Объект	Пункт меню	Назначение пункта меню
	Активировать программу	Запустить мастер создания задачи активации программы.
	Отчет о ключах	Создать и просмотреть отчет о ключах на клиентских устройствах.
Управление программами → Категории программ	**Создать → Категория**	Создать категорию программ.
Управление программами → Реестр программ	**фильтр**	Настроить фильтр для списка программ.
	Наблюдаемые программы	Настроить публикацию событий об установке программ.
	Удалить неустановленные программы	Удалить из списка информацию о программах, которые уже не установлены на устройствах сети.
Управление программами → Обновления программного обеспечения	**Принять Лицензионные соглашения обновлений**	Принять Лицензионные соглашения обновлений программного обеспечения.
Управление программами → Учет сторонних лицензий	**Создать → Группу лицензионных программ**	Создать группу лицензионных программ.
Удаленная установка → Инсталляционные пакеты	**Показать актуальные версии программ**	Просмотреть список актуальных версий программ "Лаборатории Касперского", выложенных на интернет-серверах.
	Создать → Инсталляционный пакет	Создать инсталляционный пакет.
	Все задачи → Обновить базы	Обновить базы программ в инсталляционных пакетах.
	Все задачи → Показать общий список автономных пакетов	Просмотреть список автономных пакетов установки, созданных для инсталляционных пакетов.

Объект	Пункт меню	Назначение пункта меню
Обнаружение устройств → Домены	**Все задачи → Активность устройств**	Настроить параметры реакции Сервера администрирования на отсутствие активности устройств в сети.
Обнаружение устройств → IP-диапазоны	**Создать → IP-диапазон**	Создать IP-диапазон.
Хранилища → Обновления и патчи ПО Лаборатории Касперского	**Загрузить обновления**	Открыть окно свойств задачи загрузки обновлений в хранилище Сервера администрирования.
	Параметры загрузки обновлений	Настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования.
	Отчет об используемых базах	Создать и просмотреть отчет о версиях баз.
	Все задачи → Очистить хранилище обновлений	Очистить хранилище обновлений на Сервере администрирования.
Хранилища → Оборудование	**Создать → Устройство**	Создать сетевое устройство.

Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

Таблица 75. Значение граф списка управляемых устройств

Название графы	Значение
Имя	NetBios-имя клиентского устройства. Описание значков имени устройств приведено в приложении (см. раздел "Статусы устройств, задач и политик" на стр. 862).
Тип операционной системы	Тип операционной системы клиентского устройства.
Windows-домен	Наименование Windows-домена, в котором находится клиентское устройство.
Установлен Агент	Результат установки на клиентское устройство Агента администрирования.

Название графы	Значение
Функционирует Агент	Результат функционирования Агента администрирования.
Постоянная защита	Установлена программа защиты (*Да*, *Нет*).
Соединение с Сервером	Время, прошедшее с момента соединения клиентского устройства с Сервером администрирования.
Последнее обновление	Время, прошедшее с момента последнего обновления Сервера администрирования Kaspersky Security Center.
Статус	Текущий статус клиентского устройства (*ОК, Критический, Предупреждение)*.

Название графы	Значение
Описание статуса	Причины изменения статуса клиентского устройства на *Критический* или *Предупреждение.* Статус устройства изменяется на *Предупреждение* или *Критический* по следующим причинам: • Не установлена программа защиты. • Найдено много вирусов. • Уровень постоянной защиты отличается от уровня, установленного администратором. • Давно не выполнялся поиск вирусов. • Базы устарели. • Давно не подключался. • Есть необработанные объекты. • Требуется перезагрузка. • Установлены несовместимые программы. • Обнаружены уязвимости в программах. • Давно не выполнялся поиск обновлений Windows. • Определенное состояние шифрования данных. • Параметры мобильного устройства не соответствуют политике. • Есть необработанные инциденты. • Срок действия лицензии скоро истечет. Статус устройства изменяется только на *Критический* по следующим причинам: • Срок действия лицензии истек. • Контроль над устройством потерян. • Выключена защита. • Не запущена программа защиты. Управляемые программы "Лаборатории Касперского" на клиентских устройствах могут пополнять список описаний статусов. Kaspersky Security Center может получать описание статуса клиентского устройства от управляемых программ "Лаборатории Касперского" на этом устройстве. Если статус, присвоенный устройству управляемыми программами, не совпадает со статусом, присвоенным Kaspersky Security Center, в Консоли администрирования отображается статус, наиболее критичный для безопасности устройства. Например, если одна из управляемых программ присвоила устройству статус *Критический*, а Kaspersky Security Center – статус *Предупреждение*, то в Консоли администрирования для устройства отобразится статус *Критический* и описание этого статуса от управляемой программы.

Название графы	Значение
Обновление информации	Время, прошедшее с момента последней успешной синхронизации клиентского устройства с Сервером администрирования.
Имя DNS-домена	Имя DNS-домена клиентского устройства.
DNS домен	Основной DNS-суффикс.
IP-адрес	IP-адрес клиентского устройства. Рекомендовано использовать IPv4 адрес.
Видим в сети	Продолжительность видимости клиентского устройства в сети.
Проверка по требованию	Дата и время последней проверки клиентского устройства, выполненной программой защиты по требованию пользователя.
Обнаружено вирусов	Количество обнаруженных вирусов.
Статус постоянной защиты	Статус постоянной защиты (*Запускается, Выполняется, Выполняется (максимальная защита), Выполняется (максимальная скорость), Выполняется (рекомендуемый), Выполняется (с пользовательскими параметрами), Остановлена, Приостановлена, Сбой)*.
IP-адрес соединения	IP-адрес подключения к Серверу администрирования Kaspersky Security Center.
Версия Агента администрирования	Версия Агента администрирования.
Версия защиты	Версия программы защиты, установленной на клиентском устройстве.
Версия баз	Версия антивирусных баз.
Время включения	Дата и время последнего включения клиентского устройства.
Перезагрузка	Требуется перезагрузка клиентского устройства.
Агент обновлений	Имя устройства, выполняющего роль агента обновлений для этого клиентского устройства.
Описание	Описание клиентского устройства, полученное при сканировании сети.

Название графы	Значение
Состояние WUA	Состояние Windows Update Agent клиентского устройства. Значение *Да* соответствует клиентским устройствам, которые получают обновления через Windows Update от Сервера администрирования. Значение *Нет* соответствует клиентским устройствам, которые получают обновления через Windows Update из других источников.
Разрядность операционной системы	Разрядность операционной системы клиентского устройства.
Статус защиты от спама	Статус компонента защиты от спама (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно)*.
Статус защиты данных от утечек	Статус компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно)*.
Статус защиты для серверов совместной работы	Статус компонента контентной фильтрации (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно)*.
Статус антивирусной защиты почтовых серверов	Статус компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно)*.
Статус Endpoint Sensor	Статус компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно)*.

Статусы устройств, задач и политик

В таблице ниже представлен список значков, отображающихся в дереве консоли и в рабочей области Консоли администрирования рядом с именами устройств, задач и политик. Эти значки характеризуют статус объектов.

Таблица 76. Статусы устройств, задач и политик

Иконка	Состояние
	Устройство с операционной системой для рабочих станций, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *ОК*.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Критический*.

	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с операционной системой для серверов, обнаруженное в сети и не входящий в состав какой-либо группы администрирования.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *ОК*.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Устройство с операционной системой для серверов, входящий в состав группы администрирования, со статусом *Критический*.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *ОК*.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *Предупреждение*.
	Мобильное устройство, входящее в состав группы администрирования, со статусом *Критический*.
	Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *ОК*. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *ОК*. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI не в сети.

	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI в сети. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI не в сети.
	Активная политика.
	Неактивная политика.
	Активная политика, унаследованная от группы, созданной на главном Сервере администрирования.
	Активная политика, унаследованная от группы верхнего уровня иерархии.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Ожидает выполнения* или *Завершена*.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Выполняется*.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Завершена с ошибкой*.
	Задача, унаследованная от группы, созданной на главном Сервере администрирования.
	Задача, унаследованная от группы верхнего уровня иерархии.

Значки статусов файлов в Консоли администрирования

Для упрощения работы с файлами в Консоли администрирования Kaspersky Security Center рядом с именами файлов отображаются значки (см. таблицу ниже). Значки сигнализируют о статусах, присвоенных файлам управляемыми программами "Лаборатории Касперского" на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Необработанные файлы**.

Статусы присваиваются объектам программой Kaspersky Endpoint Security, установленной на клиентском устройстве, на котором находится объект.

Таблица 77. Соответствие значков статусам файлов

Иконка	Состояние
	Файл со статусом *Заражен*.

	Файл со статусом *Предупреждение* или *Возможно зараженный.*
	Файл со статусом *Помещен в папку пользователем*.
	Файл со статусом *Ложное срабатывание*.
	Файл со статусом *Вылечен*.
	Файл со статусом *Удален*.
	Файл в папке **Карантин** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.
	Файл в папке **Резервное хранилище** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.
	Файл в папке **Необработанные файлы** со статусом *Не заражен*, *Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.

Поиск и экспорт данных

В этом разделе содержится информация о способах поиска данных и об экспорте данных.

В этом разделе

Поиск устройств

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Результаты

поиска можно сохранить в текстовом файле.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

► *Чтобы искать клиентские устройства, входящие в группу администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку группы администрирования.
2. В контекстном меню папки группы администрирования выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать нераспределенные устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать устройства независимо от того, входят они в состав групп администрирования или нет, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

В окне **Поиск** вы можете также искать группы администрирования и подчиненные Серверы администрирования с помощью раскрывающегося списка в правом верхнем углу окна. Поиск групп администрирования и подчиненных Серверов администрирования недоступен при открытии окна **Поиск** из папки **Нераспределенные устройства**.

Для поиска устройств вы можете использовать в полях ввода окна **Поиск** регулярные выражения (см. раздел "Использование регулярных выражений в строке поиска" на стр. 878).

Полнотекстовый поиск в окне **Поиск** доступен:

- на закладке **Сеть** в поле **Комментарий**;
- на закладке **Оборудование** в полях **Устройство**, **Производитель**, **Описание**.

См. также:

Параметры поиска устройств.....867

Параметры поиска устройств

Ниже представлены описания параметров поиска управляемых устройств. Результаты поиска отображаются в таблице в нижней части окна.

Сеть

На закладке **Сеть** можно настроить критерии поиска устройств на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя).

- **Windows-домен**

  Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

  - Внутри одного слова:
    - ***. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

- **?.** Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

- Для связи нескольких слов:
  - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-интервал**

  Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию флажок снят.

Теги

На закладке **Теги** можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

На закладке **Active Directory** можно настроить критерии поиска устройств на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

  Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

  По умолчанию флажок снят.

- **Включая дочерние подразделения**

  Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

На закладке **Сетевая активность** можно указать критерии поиска устройств на основании их сетевой активности:

- **Является агентом обновлений**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Есть**. В выборку будут включены устройства, являющиеся точками распространения.
- **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Есть**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Время последнего соединения с Сервером администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если флажок установлен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое

указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

По умолчанию флажок снят.

- **Устройство видимо в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Есть**. Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

Программа

На закладке **Программа** можно указать критерии поиска устройств на основании выбранной управляемой программы:

- **Название программы**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

  В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

  Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center 10**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Есть**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Установлена программа защиты**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

  - **Есть**. Программа включает в выборку устройства, на которых установлена программа безопасности.
  - **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
  - **Значение не выбрано**. Критерий не применяется.

Операционная система

На закладке **Операционная система** можно настроить критерии поиска устройств на основании установленной на них операционной системы:

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы (X.Y.)**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Статус устройства

На закладке **Статус устройства** можно указать критерии поиска устройств по статусу устройства от управляемой программы:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический*, *Предупреждение*.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический*, *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

На закладке **Компоненты защиты** можно настроить параметры поиска клиентских устройств по состоянию защиты:

- **Дата выпуска баз**

  Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию флажок снят.

- **Количество записей в базах**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

  По умолчанию флажок снят.

- **Время последнего поиска вирусов**

  Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого антивирусная проверка выполнялась в последний раз.

  По умолчанию флажок снят.

- **Количество найденных вирусов**

  Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию флажок снят.

Реестр программ

На закладке **Реестр программ** можно настроить параметры поиска устройств в

зависимости от того, какие программы на них установлены:

- **Название программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Производитель**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Искать по обновлению**

  Если флажок установлен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки флажка названия полей ввода **Название программы** и **Версия программы** меняются на **Имя обновления** и **Версия обновления**.

  По умолчанию флажок снят.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

Иерархия Серверов администрирования

На закладке **Иерархия Серверов администрирования** можно включить или отключить учет информации, хранящейся на подчиненных Серверах администрирования, во время поиска устройств:

- **Включая данные с подчиненных Серверов до уровня**

  Если флажок установлен, при поиске устройств будет учитываться информация с подчиненных Серверов администрирования.

  В поле ввода указывается уровень вложенности подчиненных Серверов администрирования, информация с которых будет учитываться при поиске устройств.

  По умолчанию флажок снят.

Виртуальные машины

На закладке Виртуальные машины можно настроить параметры поиска устройств в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

- **Есть**. Искомые устройства должны являться виртуальными машинами.
- **Нет**. Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Есть**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Оборудование

На закладке **Оборудование** можно настроить поиск клиентских устройств по установленному на них оборудованию:

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Производитель**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

  Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Частота процессора (МГц)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

  Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Уязвимости и обновления

На закладке **Уязвимости и обновления** можно настроить параметры поиска устройств по источнику обновлений Windows Update:

- **WUA переключен на Сервер администрирования**

  В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

  - **Есть**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
  - **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Пользователи

На закладке **Пользователи** можно настроить параметры поиска устройств по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если флажок установлен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если флажок установлен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Описания статусов от управляемой программы

На закладке **Описания статусов от управляемой программы** можно настроить поиск по описаниям статусов устройств от управляемой программы:

- **Описание статуса устройства**

  Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

Статусы компонентов управляемых программ

На закладке **Статусы компонентов управляемых программ** можно настроить поиск по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу защиты данных от утечек (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства*, *Приостановлена*, *Остановлена*, *Выполняется*, *Запускается*, *Сбой*).

См. также

Использование регулярных выражений в строке поиска 878

Поиск устройств 865

Использование масок в строковых переменных

Для строковых переменных допустимо использование масок. Для создания масок вы можете использовать следующие регулярные выражения:

- Знак подстановки (*) – любая строка длиной 0 или более символов.
- Вопросительный знак (?) – один любой символ.
- [<интервал>] – Заменяет один символ из заданного диапазона или множества.

  Например: [0–9] – любая цифра. [abcdef] – один из символов a, b, c, d, e, f.

Использование регулярных выражений в строке поиска

Для поиска отдельных слов и символов вы можете использовать в строке поиска следующие регулярные выражения:

- *. Заменяет последовательность любого количества символов. Например, для поиска слов "Сервер", "Серверный" или "Серверная" в строке поиска нужно ввести выражение `Сервер*`.
- ?. Заменяет любой один символ. Например, для поиска слов "Окно" или "Окна" в строке поиска нужно ввести выражение `Окн?`.

  > Текст в строке поиска не может начинаться с ?.

- [<интервал>]. Заменяет один символ из заданного диапазона или множества. Например, для поиска любой цифры в строке поиска нужно ввести выражение `[0-9]`. Для поиска одного из символов a, b, c, d, e, f в строке поиска нужно ввести выражение `[abcdef]`.

Для полнотекстового поиска вы можете использовать в строке поиска следующие регулярные выражения:

- Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами. Например, для поиска фразы, содержащей слово "Подчиненный" или "Виртуальный" (или оба этих слова), в строке поиска нужно ввести выражение `Подчиненный Виртуальный`.
- Знак "плюс" (+), AND или &&. При написании перед словом обозначает обязательное наличие слова в тексте. Например, для поиска фразы, содержащей и слово "Подчиненный", и слово "Виртуальный", в строке поиска можно ввести выражения: `+Подчиненный+Виртуальный`, `Подчиненный AND Виртуальный`, `Подчиненный && Виртуальный`.
- OR или ||. При написании между словами обозначает наличие одного или другого слова в тексте. Например, для поиска фразы, содержащей или слово "Подчиненный", или слово "Виртуальный", в строке поиска можно ввести выражения: `Подчиненный OR Виртуальный`, `Подчиненный || Виртуальный`.
- Знак "минус" (-). При написании перед словом обозначает обязательное отсутствие слова в тексте. Например, для поиска фразы, в которой должно присутствовать слово "Подчиненный", и должно отсутствовать слово "Виртуальный", нужно ввести в строке поиска выражение `+Подчиненный-Виртуальный`.
- `"<фрагмент текста>"`. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте. Например, для поиска фразы, содержащей словосочетание "Подчиненный Сервер", нужно ввести в строке поиска выражение `"Подчиненный Сервер"`.

Полнотекстовый поиск доступен в следующих блоках фильтрации:

- в блоке фильтрации списка событий по графам **Событие** и **Описание**;
- в блоке фильтрации учетных записей пользователей по графе **Имя**;
- в блоке фильтрации реестра программ по графе **Название**, если в блоке **Показывать в списке** выбран критерий фильтрации **без группировки**.

Экспорт списков из диалоговых окон

В диалоговых окнах программы вы можете экспортировать в текстовые файлы списки объектов.

Экспорт списка объектов возможен для тех разделов диалогового окна, которые содержат кнопку **Экспортировать в файл**.

Параметры задач

В этом разделе перечислены параметры задач Kaspersky Security Center.

В этом разделе

Общие параметры задач

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.
  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:
  - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Каждый N час**

Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях, начиная с указанных даты и времени.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее

системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу Поиск вирусов.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет

производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  - **Задать адреса устройств вручную или импортировать из списка**

    Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

    Вы можете использовать этот параметр для выполнения задачи для заданной

подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или сканировать устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи
  - **Учетная запись по умолчанию.**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись:**

    Поля **Учетная запись** и **Пароль** становятся доступными для изменения. Заполните эти поля, чтобы указать данные учетной записи, которая имеет необходимые права для выполнения.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль.**

    Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Дополнительные параметры расписания:
  - **Активировать устройство перед запуском задачи функцией Wake On LAN за (мин)**

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

По умолчанию параметр выключен.

- **Выключать устройство после выполнения задачи**

Устройство выключается автоматически после завершения задачи.

Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше (мин)**

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
  - Блок **Сохранять информацию о результатах**
    - **На Сервере администрирования в течение (сут)**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

- **В журнале событий ОС на клиентском устройстве**

События программы, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

По умолчанию параметр выключен.

- **В журнале событий ОС на Сервере администрирования**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранить все события**

Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события о ходе выполнения задачи.**

Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением

задачи.

- **Сохранять только результат выполнения.**

Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности
- Параметры области действия задачи

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

- **Выборка устройств**

Вы можете изменить выборку устройств, к которым применяется задача.

- **Исключения из области действия задачи**

Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**

Параметры задачи загрузки обновлений в хранилище Сервера администрирования

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского".

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.

- Главный Сервер администрирования.

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Прочие параметры**

  - **Форсировать обновление подчиненных Серверов**

Если флажок установлен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

По умолчанию параметр выключен.

  - **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями

на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступа к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не форсировать обновление устройств и подчиненных Серверов администрирования до окончания копирования**

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

- **Обновлять модули Агентов администрирования**

Если этот параметр включен, обновления для программных модулей Агента администрирования устанавливаются автоматически после того, как Сервер администрирования завершит выполнение задачи Загрузка обновлений в хранилище и обновления будут загружены в хранилище. Полученные обновления модулей Агента администрирования можно установить вручную.

По умолчанию параметр включен.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Раздел **Параметры**, блок **Состав обновлений**.
  - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. раздел "Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"" на стр. 361).

По умолчанию параметр выключен.

- Раздел **Проверка обновлений**.
  - **Выполнять проверку обновлений перед распространением**

Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу проверки обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного

хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи проверки обновлений.

По умолчанию параметр выключен.

- **Задача проверки обновлений**

Эта задача проверяет загруженные обновления перед тем как распространить их на все устройства, для которых Сервер администрирования выбран в качестве источника обновлений.

См. также:

Параметры задачи загрузки обновлений в хранилища точек распространения

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского".

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.

- Главный Сервер администрирования.

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Прочие параметры**
  - **Папка для хранения обновлений**

Папка используется только для загрузки обновлений. Укажите локальную папку на устройствах, которые назначены точками распространения. Вы можете использовать системные переменные.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Раздел **Параметры**, блок **Состав обновлений**.
  - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. раздел "Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"" на стр. 361).

По умолчанию параметр выключен.

См. также:

Общие параметры задач 879

Создание задачи загрузки обновлений в хранилища точек распространения 368

Параметры задачи поиска уязвимостей и требуемых обновлений

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Использовать данные служб Windows Server Update Services**

При поиске уязвимостей и программ, для которых требуются обновления, Kaspersky Security Center использует информацию о применимых обновлениях Microsoft Windows из источника обновлений Microsoft.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Подключаться к серверу обновлений для получения новых данных**

Если этот параметр включен, Kaspersky Security Center подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Kaspersky Security Center использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Поэтому рекомендуется выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах обновлений Windows.

По умолчанию параметр включен.

- **Использовать список программ, предоставленный "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств.Утилита удаленной диагностики Kaspersky Security Center" на стр. 608), с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в

соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

Максимальный объем дискового пространства в мегабайтах (МБ), который может быть занят файлами расширенной диагностики.

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

См. также:

Общие параметры задач 879

Поиск уязвимостей в программах 403

Параметры задачи установки требуемых обновлений и закрытия уязвимостей

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Укажите правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений (см. стр. 423).

- **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии программы при обновлении**

Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая**

Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке

%WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. раздел "Удаленная диагностика клиентских устройств).Утилита удаленной диагностики Kaspersky Security Center" на стр. 608), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

Максимальный объем дискового пространства в мегабайтах (МБ), который может быть занят файлами расширенной диагностики.

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Обновления для установки

  В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.

- Пробная установка обновлений:

  - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
  - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.
  - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
  - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

См. также:

Глобальный список подсетей

В этом разделе приведена информация и глобальном списке подсетей, которые вы можете использовать в правилах.

Чтобы сохранить информацию о подсетях вашей сети, вы можете настроить глобальный список подсетей для каждого Сервера администрирования. Этот список позволит сопоставить пары {IP-адрес, маска} и физические единицы, такие как офисы филиалов. Вы можете использовать подсети из этого списка в сетевых правилах и параметрах.

В этом разделе

Добавление подсети в глобальный список подсетей

Вы можете добавлять подсети и их описание в глобальный список подсетей.

► *Чтобы добавить подсеть в глобальный список подсетей, выполните следующие действия:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** перейдите в раздел **Глобальный список подсетей**.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Новая подсеть**.
5. Заполните следующие поля:
   - **Адрес подсети**

     IP-адрес подсети, которую вы добавляете.

- **Маска подсети**

  Маска подсети, которую вы добавляете.

- **Имя.**

  Имя подсети. Имя подсети должно быть уникальным для всего глобального списка подсетей. Если вы указали имя подсети, которое уже существует в списке, то ей будет добавлен индекс, например: ~~1, ~~2.

- **Описание**

Описание может содержать дополнительную информацию, например, о филиале, которому принадлежит эта подсеть. Этот текст возникает везде, где отображается список подсетей, например, в списке правил ограничения трафика.

Это поле не обязательно для заполнения и может быть пустым.

1. Нажмите на кнопку **ОК**.

Подсеть появится в списке подсетей.

Просмотр и изменение свойств подсети в глобальном списке подсетей

Вы можете просматривать и изменять свойства подсетей в глобальном списке подсетей.

► *Чтобы просмотреть или изменить свойства подсети в глобальном списке подсетей, выполните следующие действия:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** выберите раздел **Глобальный список подсетей**.
4. В списке выберите требуемую подсеть.
5. Нажмите на кнопку **Свойства**.

   Откроется окно **Новая подсеть**.
6. Если необходимо, измените параметры подсети (см. раздел "Добавление подсети в глобальный список подсетей" на стр. 895).
7. Нажмите на кнопку **ОК**.

Если вы сделали изменения, то они будут сохранены.

Сравнение параметров Агента администрирования для различных операционных систем (Windows, Mac и Linux)

Возможности Агента администрирования зависят от операционной системы устройства. Свойства политики Агента администрирования (см. раздел "Параметры политики Агента администрирования" на стр. 624) и

инсталляционного пакета (см. раздел "Параметры инсталляционного пакета Агента администрирования" на стр. 143) зависят от операционной системы.

Таблица 78. Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Mac	Linux
Установка			
Автоматическое создание инсталляционного пакета Агента администрирования, после установки Kaspersky Security Center (см. раздел "Инсталляционные пакеты" на стр. 111).	+	Нет	Нет
Принудительная установка с помощью соответствующих параметров задачи удаленной установки программ Kaspersky Security Center (см. раздел "Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center" на стр. 117).	+	+	+
Установка программ с помощью рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center (см. раздел "Запуск автономных пакетов, сформированных Kaspersky Security Center" на стр. 119).	+	+	+
Установка путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами (см. раздел "Развертывание захватом и копированием образа жесткого диска устройства" на стр. 113).	+	Нет	+
Установка программ с помощью сторонних средств удаленной установки программ (см. раздел "Развертывание при помощи сторонних средств удаленной установки приложений" на стр. 112).	+	+	+

Функция Агента администрирования	Windows	Mac	Linux
Установка вручную с помощью запуска инсталляторов программ на устройствах (см. раздел "Возможности ручной установки приложений" на стр. 119).	+	+	+
Установка Агента администрирования в неинтерактивном режиме (см. раздел "Установка в тихом режиме (с файлом ответов)" на стр. 125).	+	+	+
Установка Агента администрирования в неинтерактивном режиме (см. стр. 140)	+	Нет	Нет
Подключение клиентского устройства к Серверу администрирования вручную (см. стр. 587)	+	+	+
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (см. раздел "Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center" на стр. 457).	+	Нет	Нет
Автоматическое распространение ключа (см. раздел "Автоматическое распространение лицензионного ключа" на стр. 299)	+	+	+
Принудительная синхронизация (на стр. 598)	+	+	+
Точка распространения			
Использование точки распространения (см. раздел "О точках распространения" на стр. 86)	+	+	+
Автоматическое назначение точек распространения (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 88)	+	+	+
Офлайн-модель получения обновлений (см. стр. 438)	+	+	+
Работа с другими программами			

Функция Агента администрирования	Windows	Mac	Linux
Удаленная установка программ на устройства (см. раздел "Удаленная установка приложений на устройства с установленным Агентом администрирования" на стр. 120)	+	Нет	Нет
Обновления программного обеспечения (на стр. 427)	+	Нет	Нет
Настройка обновлений операционной системы в политике Агента администрирования (см. раздел "Настройка обновлений Windows в политике Агента администрирования" на стр. 454)	+	Нет	Нет
Просмотр информации об уязвимостях в программах (см. стр. 402)	+	+	+
Поиск уязвимостей в программах (на стр. 403)	+	+	+
Инвентаризация программного обеспечения, установленного на устройствах (см. раздел "Изменение времени начала инвентаризации программного обеспечения" на стр. 400)	+	Нет	Нет
Просмотр реестра программ (на стр. 397)	+	Нет	Нет
Виртуальные машины			
Установка Агента администрирования на виртуальные машины (см. раздел "Виртуальная инфраструктура" на стр. 134)	+	Нет	+
Оптимизация параметров для VDI (см. раздел "Рекомендации по снижению нагрузки на виртуальные машины" на стр. 134)	+	+	+
Поддержка динамических виртуальных машин (см. стр. 135)	+	+	+
Другое			
Аудит действий на удаленном клиентском устройстве (см. стр. 592)	+	Нет	Нет

Функция Агента администрирования	Windows	Mac	Linux
Мониторинг состояния антивирусной защиты (см. раздел "Отслеживание состояния антивирусной защиты с помощью информации в системном реестре" на стр. 530)	+	Нет	Нет
Управление перезагрузкой устройств (см. раздел "Настройка перезагрузки клиентского устройства" на стр. 591)	+	Нет	Нет
Поддержка отката файловой системы (см. раздел "Поддержка отката файловой системы для устройств с Агентом администрирования" на стр. 136)	+	+	+
Использование Агента администрирования в качестве шлюза соединений (см. раздел "Использование точки распространения в качестве шлюза соединений" на стр. 538)	+	+	+
Менеджер соединений (см. раздел "О расписании соединений" на стр. 598)	+	+	+
Переключение Агента администрирования на другой Сервер администрирования (см. раздел "Автономные пользователи" на стр. 577)	+	Нет	Нет
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk" на стр. 593)	+	+	+
Удаленное подключение к рабочему столу клиентского устройства (см. стр. 589)	+	Нет	Нет

Приложение. Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения выводит программу из безопасного состояния.

Таблица 79. Параметры и их значения для программы в сертифицированном состоянии

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Месторасположение папки общего доступа	При установке Kaspersky Security Center папка общего доступа по умолчанию называется KLSHARE и расположена <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.	Не в папке, где установлен Сервер администрирования Kaspersky Security Center.
Политики	Для каждой управляемой программы создана политика.	
Пароль на деинсталляцию Агента администрирования	В политике Агента администрирования установлен пароль на удаление Агента администрирования. Возможные значения: • установлен; • снят.	Установлен.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Защита паролем политики Kaspersky Endpoint Security для Windows. Параметр программы Kaspersky Endpoint Security для Windows, если эта программа установлена.	Защита паролем позволяет установить ограничение на управление всеми или отдельными функциями и параметрами Kaspersky Endpoint Security для Windows, снижая вероятность несанкционированного или непреднамеренного внесения изменений в работу программы. Возможные значения: • установлена; • снята.	Установлена.
Автоматическое обновление модулей Агентов администрирования	Обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования (или точки распространения) завершает задачу получения обновлений. Возможные значения: • включен; • выключен.	Выключен.
Установка применимых обновлений со статусом одобрения *Не определено*	Патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Возможные значения: • включен; • выключен.	Выключен.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Запуск задачи **Загрузка обновлений в хранилище Сервера администрирования**	Задача **Загрузка обновлений в хранилище** выполняет загрузку обновлений баз и программных модулей, которые копируются с источника обновлений и размещаются в папке общего доступа. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически по расписанию. Рекомендуемый интервал запуска задачи – один раз в час.
Запуск задачи **Установка обновлений**	Задача **Установка обновлений** выполняет установку ранее загруженных в хранилище обновлений на клиентские устройства. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически, по завершении задачи **Загрузка обновлений в хранилище**.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Передача данных сервису KSN	Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Возможные значения передачи данных программы сервису KSN: • отключена; • включена.	Отключена.
Источник обновлений задач **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**	Источник обновлений баз и модулей управляемых программ "Лаборатории Касперского". Возможные значения: • Серверы обновлений "Лаборатории Касперского"; • Главный Сервер администрирования; • Локальная или сетевая папка.	• Главный Сервер администрирования; • Локальная или сетевая папка. Источник обновлений *Серверы обновлений "Лаборатории Касперского"* удален, чтобы программа не передавала информацию на серверы обновлений "Лаборатории Касперского".

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Способ активации Сервера администрирования	Возможные значения: • с помощью файла ключа; • с помощью кода активации.	С помощью файла ключа.
Служба прокси-сервера активации "Лаборатории Касперского"	Служба прокси-сервера активации "Лаборатории Касперского" используется для обеспечения передачи запросов на активацию от управляемых программ к серверам активации "Лаборатории Касперского". Возможные значения: • отключена; • включена.	Отключена
Доверенные каналы с использованием SSL-протокола	Протокол SSL позволяет идентифицировать стороны, взаимодействующие при подключении (взаимодействие между Севером администрирования и устройствами), осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. Возможные значения: • используется; • не используется.	Используется.
Права пользователей	Права обеспечивают доступ администраторов, пользователей и групп пользователей к разным функциям программы.	Минимально необходимые права настроены: только уполномоченные роли имеют права изменять параметры защиты.
Условия для статуса *Критический*	Набор условий при котором устройство принимает статус *Критический*.	Выбрано условие **Найдено много вирусов**. Параметр **Более чем** равен значению 0.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Максимальное количество событий, хранящихся в базе данных Сервера администрирования	Максимальное количество событий, которое хранится в базе данных Сервера администрирования, необходимое для проведения аудита программы.	Рекомендуется установить значение не меньше 400 000 событий.
Срок хранения событий	Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита программы.	Рекомендуется установить значения: • Для событий с уровнем важности *Критические* – не меньше 180 дней. • Для событий с уровнем важности *Предупреждение* – не меньше 90 дней. • Для событий с уровнем важности *Информационное сообщение* – не меньше 30 дней.
Срок хранения ревизий изменений объектов	Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита программы.	Рекомендуется установить значение не меньше 90 дней.
Права доступа к возможностям шифрования	Права доступа пользователей и ролей пользователей к возможностям шифрования данных.	Запрещено.
Программа Kaspersky Security Center 11 Web Console	Программа (веб-приложение), работающая совместно с программой Kaspersky Security Center 11 и предназначенную для контроля состояния системы безопасности сетей организации, находящихся под защитой программ “Лаборатории Касперского”.	Не установлена.

См. также

Настройка эталонных значений параметров программы

Этот раздел содержит инструкции по установке эталонных значений параметров программы. Настройка программы по эталонным параметрам необходима для работы сертифицированной конфигурации программы.

Месторасположение папки общего доступа Сервера администрирования

Измените месторасположение папки общего доступа Сервера администрирования. Папка должна находиться не в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа при установке Сервера администрирования, выполните следующие действия:*

1. Запустите установку Сервера администрирования (см. раздел "Установка Kaspersky Security Center" на стр. 177).
2. В окне **Папка общего доступа** мастера установки измените путь к папке общего доступа (см. раздел "Шаг 11.Определение папки общего доступа" на стр. 198).

► *Чтобы изменить папку общего доступа установленного Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Папка общего доступа** измените расположение папки общего доступа.

Политики

Настройте активные политики для каждой управляемой программы "Лаборатории Касперского" для всех групп администрирования, в том числе политику Агента администрирования и политику Kaspersky Endpoint Security для Windows. Для политики Агента администрирования необходимо установить пароль на удаление программы Агента администрирования. Для политики Kaspersky Endpoint Security для Windows необходимо настроить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows.

Пароль на деинсталляцию Агента администрирования

► *Чтобы установить пароль на удаление программы Агента администрирования, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Агент администрирования выберите пункт **Свойства**.
3. В окне свойств политики в разделе **Параметры** выберите установите флажок **Использовать пароль деинсталляции**.
4. Нажмите на кнопку **Изменить**.
5. В окне **Изменения пароля** введите пароль.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Защита паролем политики Kaspersky Endpoint Security для Windows

► *Чтобы установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.
3. В окне свойств политики в разделе **Дополнительные параметры** выберите подраздел **Параметры программы**.
4. В разделе **Параметры программы** в блоке **Защита паролем** нажмите на кнопку **Настроить**.
5. В окне **Защита паролем** установите флажок **Включить защиту паролем**.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Автоматическое обновление модулей Агентов администрирования

По умолчанию обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Отключите автоматическое обновление модулей Агента администрирования. Сертификации подлежат только определенные версии исполняемых модулей программы.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.

3. В контекстном меню задачи выберите пункт **Свойства**.
4. В окне свойств задачи выберите раздел **Параметры**.
5. В подразделе **Прочие параметры** перейдите по ссылке **Настроить**.

   Откроется окно **Прочие параметры**.
6. Снимите флажок **Обновлять модули Агентов администрирования**.

   Если флажок снят, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
7. Нажмите на кнопку **ОК**.

Если в сети вашей организации назначены точки распространения, то для всех точек распространения также требуется отключить автоматическое обновление модулей Агента администрирования.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы точкой распространения, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** выберите задачу **Загрузка обновлений в хранилища точек распространения**.
3. В контекстном меню задачи выберите пункт **Свойства**.
4. В окне свойств задачи выберите раздел **Параметры**.
5. В подразделе **Прочие параметры** перейдите по ссылке **Настроить**.
6. Откроется окно **Прочие параметры**.
7. Снимите флажок **Обновлять модули Агентов администрирования**.

   Если флажок снят, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
8. Нажмите на кнопку **ОК**.

Установка применимых обновлений со статусом одобрения "Не определено"

1. По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Отключите автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

► *Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения* Не определено, выполните следующие действия:

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агент администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.
4. В разделе свойств политики **Управление патчами и обновлениями** снимите флажок **Устанавливать**

применимые обновления со статусом одобрения "Не определено".

Если флажок **Устанавливать применимые обновления со статусом одобрения "Не определено"** снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

5. Нажмите на кнопку **ОК**.

Запуск задачи Загрузка обновлений в хранилище

Настройте автоматический запуск задач **Загрузка обновлений в хранилище** и **Установка обновлений**.

Рекомендуемый интервал автоматического запуска задачи Сервера администрирования **Загрузка обновлений в хранилище** составляет один раз в час.

► *Чтобы настроить автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище** один раз в час, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Загрузка обновлений в хранилище** выберите пункт **Свойства**.
3. В окне свойств перейдите в раздел **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.
5. В поле **Интервал запуска (ч)** установите значение 1.
6. Нажмите на кнопку **ОК**.

Запуск задачи Установка обновлений

Настройте запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище**.

► *Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище**, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Установка обновлений** выберите пункт **Свойства**.
3. В окне свойств перейдите в раздел **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **По завершении другой задачи**.
5. В поле **Название задачи** выберите значение **Загрузка обновлений в хранилище**.
6. В поле **Результат выполнения** выберите значение **Завершена успешно**.
7. Нажмите на кнопку **ОК**.

Передача данных сервису KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость

реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний (см. раздел "О KSN и KPSN" на стр. 735).

Для работы программы в сертифицированной конфигурации службы, которые связаны с отправкой данных на внешние сервера и получением команд от внешних серверов (за периметром сети организации), должны быть отключены. Отключите передачу данных программой сервису KSN.

► *Чтобы отключить передачу данных сервису KSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно отключить передачу данных к сервису KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".
5. Снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.
6. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

► *Чтобы отключить передачу данных сервису KSN точкой распространения, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно отключить передачу данных к сервису KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Точки распространения**.
4. Выберите точку распространения и нажмите на кнопку Свойства.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
6. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".
7. Снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить

службу прокси-сервера KSN.

8. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от точки распространения и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

Передача данных сервису KSN должна быть отключена во всех управляемых программах.

Альтернативой отказу от использования KSN может стать использование Локального KSN (см. раздел "Настройка доступа к KPSN" на стр. 736). В этом случае вы получите доступ к оперативной базе знаний "Лаборатории Касперского", но информация о работе программ "Лаборатории Касперского" не будет передаваться на сервера "Лаборатории Касперского".

Источник обновлений задачи Загрузка обновлений в хранилище

Отключите передачу данных программой сервису обновлений "Лаборатории Касперского". Для этого необходимо удалить серверы обновлений "Лаборатории Касперского" в задачи Загрузка обновлений в хранилище из источников обновлений.

► *Чтобы удалить серверы обновлений "Лаборатории Касперского" в задаче Загрузка обновлений в хранилище из источников обновлений, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Загрузка обновлений в хранилище** выберите пункт **Свойства**.
3. В окне свойств задачи перейдите в раздел **Параметры**.
4. В подразделе **Источники обновлений** перейдите по ссылке **Настроить**.
5. В окне **Источники обновлений** удалите значение *Серверы обновлений "Лаборатории Касперского"*.

Настройку необходимо выполнить для задачи **Загрузка обновлений в хранилище** Сервера администрирования и для всех агентов обновлений.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации программы с помощью кода активации программа регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа.

Способ активации Сервера администрирования

Сервер администрирования необходимо активировать с помощью файла ключа.

► *Чтобы активировать Сервер администрирования с помощью файла ключа, выполните следующие*

действия:

1. В дереве консоли выберите Сервер администрирования, который вы хотите активировать.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер первоначальной настройки**.
3. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.
4. В окне мастера **Активация программы** укажите файл ключа, на основании которого ключ будет добавлен в программу.

Служба прокси-сервера активации "Лаборатории Касперского"

Рекомендуется отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского", выполните следующие действия:*

1. Откройте список служб вашего устройства.
2. Выберите в списке службу прокси-сервера активации "Лаборатории Касперского".
3. В контекстном меню службы выберите раздел **Свойства**.
4. В окне свойства службы на закладке **Общие** в поле **Тип запуска** выберите значение **Отключена**.
5. Нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

Доверенные каналы с использованием SSL-протокола

Настройте использование SSL-соединений для гарантированной доставки информации по доверенному каналу. В сертифицированной конфигурации программа должна использовать только доверенные каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования, выполните следующие действия:*

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агента администрирования.
3. В контекстном меню политики Агента администрирования выберите пункт **Свойства**.
4. В окне свойств Агента администрирования свойств в разделе **Сеть** выберите вложенный раздел **Сеть**.
5. Установите флажок **Использовать SSL-соединение**.

6. Нажмите на кнопку **ОК**.

   Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

7. В разделе **Подключения** выберите профиль подключения и нажмите на кнопку Свойства.
8. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.

   Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.

9. Нажмите на кнопку **ОК**.

Права пользователей

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в программе. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей, выполните следующие действия:*

1. В дереве консоли выберите узел с именем необходимого Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которым нужно присвоить роль.

   Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.

   При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.

5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.

6. В окне **Роли пользователей** выберите роль для группы пользователей.
7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования

Условия для статуса "Критический"

Настройте изменение статуса устройства на *Критический* при обнаружении на нем хотя бы одного вируса.

► *Чтобы настроить изменение статуса устройства на* Критический, *выполните следующие действия:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств перейдите в раздел **Статус устройства**.
3. В блоке **Условия для статуса Критический** установите флажок для условия **Найдено много вирусов**.
4. Для условия **Найдено много вирусов** установите значение *Более чем 0*.
5. Нажмите на кнопку **ОК**.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования

Установите максимальное количество событий, хранящихся в базе данных Сервера администрирования, необходимое для проведения аудита программы. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить максимальное количество событий, хранящихся на Сервере.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Хранение событий**.
4. В поле **Максимальное количество событий, хранящихся в базе данных** установите рекомендуемое значение, не меньше 400 000 событий.

По умолчанию емкость базы данных Сервера администрирования составляет 400.000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые.

Срок хранения событий

Настройте срок хранения событий в базе данных Сервера администрирования, необходимый для проведения аудита программы.

► *Чтобы изменить срок хранения событий, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Настройка событий**.

4. Установите время хранения событий по уровню их важности:
   - На закладке **Критическое событие** установите необходимое значение (не меньше 180 дней).
   - На закладке **Предупреждение** установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий можно настроить также в свойствах политики Сервера администрирования.

► *Чтобы настроить срок хранения событий в свойствах политики Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств политики Сервера администрирования перейдите в раздел **Настройка событий**.
4. Установите время хранения событий, в зависимости от уровня важности событий:
   - На закладке **Критическое событие** установите значение не меньше 180 дней.
   - На закладке **Предупреждение** установите значение не меньше 90 дней.
   - На закладке **Информационное сообщение** установите значение не меньше 30 дней.
5. Нажмите на кнопку **ОК**.

Срок хранения ревизии изменений объектов

Настройте срок хранения ревизии объектов, необходимый для проведения аудита программы. Рекомендуемый срок хранения ревизии изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита программы.

► *Чтобы изменить срок хранения ревизии изменения объектов, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого необходимо настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Хранение истории ревизий**.
4. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.
5. Нажмите на кнопку **ОК**.

Права доступа к возможностям шифрования

Настройте запрет доступа к возможностям шифрования данных для всех ролей и пользователей.

► *Чтобы запретить доступ роли к возможностям шифрованию данных, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого необходимо настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Роли пользователей**.
4. Выберите роль и нажмите на кнопку **Изменить**.
5. В окне свойств роли пользователей перейдите в раздел **Права**.
6. В блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранной запрещено.

► *Чтобы запретить доступ пользователя к возможностям шифрованию данных, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого необходимо настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Безопасность**.
4. Выберите пользователя и перейдите на закладку **Права**.
5. На закладке **Права** в блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранного пользователя запрещено.

Уважаемый пользователь!

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

Документ может быть изменен без предварительного уведомления.

Дата редакции документа: 18.06.2019

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center.

В этом разделе

Об этом руководстве

Руководство по масштабированию Kaspersky Security Center 11 (далее "Kaspersky Security Center") адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

Все рекомендации и расчеты приведены для сетей, в которых Kaspersky Security Center управляет защитой устройств с установленным программным обеспечением "Лаборатории Касперского", в том числе мобильных. Если мобильные устройства, или любые другие управляемые устройства, необходимо рассматривать отдельно, это специально оговаривается.

Для достижения и сохранения оптимальной производительности при различных условиях работы вы должны учитывать количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center.

В руководстве приведена следующая информация:

- Ограничения Kaspersky Security Center
- о расчетах для ключевых узлов Kaspersky Security Center – Серверов администрирования и точек распространения;
    - об аппаратных требованиях к Серверам администрирования и к точкам распространения;
    - о расчете количества и иерархии Серверов администрирования;
    - о расчетах количества и конфигурации точек распространения;

- о настройке параметров сохранения событий в базе данных в зависимости от числа устройств в сети;
- о настройке параметров некоторых задач для обеспечения оптимальной производительности Kaspersky Security Center;
- о потреблении трафика (нагрузке на сеть) между Сервером администрирования Kaspersky Security Center и каждым защищаемым устройством.

Рекомендуется обращаться к этому руководству в следующих ситуациях:

- при планировании ресурсов перед установкой Kaspersky Security Center;
- при планировании существенных изменений размеров сети, в которой развернут Kaspersky Security Center;
- при переходе от тестового режима использования Kaspersky Security Center на маленьком участке сети к полноценному использованию Kaspersky Security Center в сети организации;
- при изменениях в наборе используемых функций Kaspersky Security Center.

Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

Таблица 80. Ограничения Kaspersky Security Center

Тип ограничения	Значение
Максимальное количество управляемых устройств на один Сервер администрирования	100 000
Максимальное количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования**	300
Максимальное количество групп администрирования	10 000
Максимальное количество хранимых событий	45 000 000
Максимальное количество политик	2000
Максимальное количество задач	2000

Тип ограничения	Значение
Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности)	1 000 000
Максимальное количество профилей в политике	100
Максимальное количество подчиненных Серверов у одного главного Сервера администрирования	500
Максимальное количество виртуальных Серверов администрирования	500
Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные (стационарные) устройства)	10 000
Максимальное количество устройств, которые могут использовать один шлюз соединения	10 000, включая мобильные устройства
Максимальное количество мобильных устройств на один Сервер администрирования	100 000 минус количество стационарных управляемых устройств

Расчеты для Серверов администрирования

В этом разделе приведены аппаратные и программные требования для устройств, которые используются в качестве Серверов администрирования. Также даны рекомендации для расчета количества Серверов администрирования и их иерархии, в зависимости от конфигурации сети организации.

В этом разделе

Расчет аппаратных ресурсов для Сервера администрирования

В этом разделе приведены расчеты, которыми можно руководствоваться при планировании аппаратных ресурсов для Сервера администрирования. Отдельно приводится рекомендация по расчету места на диске при использовании Системного администрирования.

В этом разделе

Аппаратные требования для СУБД и Сервера администрирования

В таблицах ниже приведены минимальные аппаратные требования СУБД и Сервера администрирования, полученные в ходе тестирования. Полный список поддерживаемых операционных систем и СУБД см. в перечне аппаратных и программных требований (см. стр. 23).

Сервер администрирования и SQL-сервер на разных устройствах, в сети 50 000 устройств

Таблица 81. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	4 ядер, 2500 МГц
ОЗУ	8 ГБ
Жесткий диск	300 ГБ, желателен RAID
Сетевой адаптер	1 Гбит

Таблица 82. Конфигурация устройства с SQL-сервером

Оборудование	Значение
Процессор	4 ядер, 2500 МГц
ОЗУ	16 ГБ
Жесткий диск	200 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 50 000 устройств

Таблица 83. Конфигурация устройства с Сервером администрирования и SQL-сервером

Оборудование	Значение
Процессор	8 ядер, 2500 МГц

Оборудование	Значение
ОЗУ	16 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Сервер администрирования и SQL-сервер на одном устройстве, в сети 100 000 устройств

Таблица 84. Конфигурация устройства с Сервером администрирования

Оборудование	Значение
Процессор	8 ядер, 2,13 ГГц
ОЗУ	8 ГБ
Жесткий диск	1 ТБ, RAID
Сетевой адаптер	1 Гбит

Таблица 85. Конфигурация устройства с SQL Server

Оборудование	Значение
Процессор	8 ядер, 2,53 ГГц
ОЗУ	26 ГБ
Жесткий диск	500 ГБ SATA RAID
Сетевой адаптер	1 Гбит

Тестирование проводилось со следующими настройками:

- на Сервере администрирования включено автоматическое назначение точек распространения, либо точки распространения назначены вручную по рекомендуемой таблице (см. раздел "Расчет количества и конфигурации точек распространения" на стр. 88);
- задача резервного копирования сохраняет резервные копии на файловый ресурс, расположенный на отдельном сервере (см. раздел "Резервное копирование и восстановление параметров Сервера администрирования" на стр. 561).
- период синхронизации Агентов администрирования настроен в соответствии с таблицей ниже.

Таблица 86. Период синхронизации Агентов администрирования

Период синхронизации, минуты	Количество управляемых устройств
15	10 000

Период синхронизации, минуты	Количество управляемых устройств
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Расчет места в базе данных

Место, которое будет занято в базе данных, можно приблизительно оценить по следующей формуле:

(200 * C + 2.3 * E + 2.5 * A), КБ,

где:

- "C" – количество устройств.
- "E" – количество сохраняемых событий (см. раздел "Скорость заполнения событиями базы данных" на стр. 931).
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетные записи пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

  Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Если вы планируете включить в параметрах политики Kaspersky Endpoint Security информирование Сервера администрирования о запускаемых программах, то для хранения информации о запускаемых программах в базе данных дополнительно потребуется (0,03 * C) ГБ.

Если Сервер администрирования распространяет обновления Windows (играет роль Windows Server Update Services), то в базе данных дополнительно потребуется 2,5 ГБ.

В ходе работы в базе данных всегда образуется так называемое *незанятое пространство* (unallocated space). Поэтому реальный размер файла базы данных (по умолчанию файл KAV.MDF в случае использования СУБД "SQL Server") часто оказывается примерно в два раза больше, чем занятое в базе данных место.

Не рекомендуется явно ограничивать размер журнала транзакций (по умолчанию файл KAV_log.LDF, если вы используете SQL Server в качестве СУБД). Рекомендуется оставить значение параметра MAXSIZE по умолчанию. Если вам необходимо ограничить размер этого файла, нужно учесть, что необходимое значение параметра MAXSIZE для KAV_log.LDF составляет 20480 МБ.

Расчет места на диске (с учетом и без учета использования Системного администрирования)

Расчет места на диске без учета использования Системного администрирования

Место на диске Сервера администрирования, требуемое для папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, можно приблизительно оценить по формуле:

(220,0 * C + 0.15 * E + 0.17 * A), КБ

где:

- "C" – количество устройств.
- "E" – количество сохраняемых событий.
- "A" – суммарное количество объектов Active Directory:
  - учетных записей устройств;
  - учетные записи пользователей;
  - учетных записей групп безопасности;
  - подразделений Active Directory.

Если сканирование Active Directory выключено, то "A" следует считать равным нулю.

Расчет дополнительного места на диске с учетом использования Системного администрирования

- Обновления. В папке общего доступа требуется дополнительно не менее 4 ГБ для хранения обновлений.
- Инсталляционные пакеты. При наличии на Сервере администрирования инсталляционных пакетов в папке общего доступа дополнительно потребуется количество места, равное суммарному размеру устанавливаемых имеющихся инсталляционных пакетов.
- Задачи удаленной установки. При наличии на Сервере администрирования задач удаленной установки на диске дополнительно потребуется количество места на диске (в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), равное суммарному размеру устанавливаемых инсталляционных пакетов.
- Патчи. Если Сервер администрирования используется для установки патчей, то потребуется дополнительное место на диске:
  - Папка для хранения патчей должна иметь объем дискового пространства, равный суммарному размеру всех загруженных патчей. По умолчанию патчи хранятся в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (вы можете назначить для хранения патчей другую папку при помощи утилиты klsrvswch). Если Сервер администрирования используется в качестве WSUS, то рекомендуется зарезервировать под эту папку не менее 100 ГБ.
  - В папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit – количество места, равное суммарному размеру тех патчей, на которые ссылаются имеющиеся экземпляры задачи установки обновлений (патчей) и закрытия уязвимостей.

Расчет количества и конфигурации Серверов администрирования

Чтобы снизить нагрузку на главный Сервер администрирования, вы можете назначить в каждую группу администрирования отдельный Сервер администрирования. Количество Серверов администрирования, подчиненных главному Серверу, не может превышать 500.

Рекомендуется выстраивать конфигурацию Серверов администрирования в зависимости от того, как устроена сеть в вашей организации. Типовые конфигурации описаны в соответствующем разделе справки (см. раздел "Типовые конфигурации Kaspersky Security Center" на стр. 79).

Расчеты для точек распространения и шлюзов соединений

В этом разделе приведены аппаратные требования к устройствам, которые используются в качестве точек распространения, и рекомендации по расчету количества точек распространения и шлюзов соединений в зависимости от конфигурации сети организации.

В этом разделе

Требования для точки распространения

Чтобы обрабатывать до 10 000 клиентских устройств, точка распространения должна отвечать следующим требованиям (предоставлена конфигурация тестового стенда):

- Процессор: Intel® Core™ i7-7700 CPU, 3.60ГГц, 4 ядра.
- ОЗУ: 8 ГБ.
- Диск: Intel SSDSC2KW120H6.

Кроме того, точка распространения должна иметь доступ в интернет и должна быть всегда включена.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения дополнительно

потребуется дисковое пространство, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

Использование специально выделенных точек распространения

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске (см. раздел "Требования для точки распространения" на стр. 842), их не отключают регулярно и на них выключен "спящий режим".

Таблица 87. Число уникально назначенных точек распространения в сети, содержащей один сегмент, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Таблица 88. Число уникально назначенных точек распространения в сети, содержащей несколько сегментов, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 100	1
Более 100	Приемлемо: (N/10000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Таблица 89. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом из сегментов сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Таблица 90. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10 – 30	1
31 – 300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

См. также:

Типовая конфигурация:Множество небольших изолированных офисов 81

Расчет количества шлюзов соединений

Если вы планируете использовать шлюз соединений, рекомендуется использовать выделенное устройство для этой функции.

Один шлюз соединений обслуживает не более 10 000 управляемых устройств, включая мобильные устройства.

Расчеты, связанные с хранением событий в базе данных

В этом разделе приведены расчеты, связанные с хранением событий в базе данных Сервера администрирования, и даны рекомендации, как минимизировать количество событий и таким образом снизить нагрузку на Сервер администрирования.

В этом разделе

Скорость заполнения событиями базы данных

В этом разделе приведены примеры скорости заполнения базы данных Сервера администрирования событиями, возникающими в работе управляемых программ.

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования.

В базу данных поступает (Ne*Nh) событий в день (см. таблицу ниже). Здесь Nh – количество клиентских устройств, на которых установлены управляемые программы. Ne – количество событий в день, информацию о которых передает с клиентского устройства установленная на нем управляемая программа Kaspersky Endpoint Security для Windows. По умолчанию Kaspersky Endpoint Security для Windows (версии 10 и 11) при штатной работе передает в базу данных около 20 событий в день. Максимальное количество событий, которое может обработать Kaspersky Security Center, составляет 2 000 000 событий в день.

Таблица 91. Скорость заполнения событиями базы данных (при штатной работе)

Количество устройств, на которых установлена программа Kaspersky Endpoint Security	Количество событий, передаваемое в базу данных в день
100	до 2 000
1 000	до 20 000
10 000	до 200 000
100 000	до 2 000 000

Максимальное количество событий, хранящихся в базе данных, определяется в разделе **Хранилище событий** окна свойств Сервера администрирования. По умолчанию в базе данных хранится не более 400 000 событий.

Хранение информации о событиях для задач и политик

По умолчанию в свойствах каждой задачи и каждой политики указано сохранение в журнале всех событий, связанных с выполнением задачи и применением политики.

Однако если задача запускается достаточно часто (например, более одного раза в неделю) и на достаточно большом количестве устройств (например, более 10 000), количество событий может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется указать в свойствах задачи один из двух других вариантов:

- **Сохранять события о ходе выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о запуске задачи, о ее ходе и о ее

выполнении (успешном, с предупреждением либо с ошибкой).

- **Сохранять только результат выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о выполнении задачи (успешном, с предупреждением либо с ошибкой).

Если политика определена для достаточно большого количества устройств (например, более 10 000), количество событий также может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения важных событий большим количеством событий об изменении состояния групповых задач.

Вы также можете уменьшить срок хранения событий, связанных с задачей (политикой). По умолчанию этот срок составляет семь дней для событий, связанных с задачей, и 30 дней для событий, связанных с политикой. При изменении срока хранения событий принимайте в расчет порядок работы, принятый в вашей организации, и количество времени, которое системный администратор может уделять анализу каждого события.

Вносить изменения в параметры хранения событий целесообразно в любом из следующих случаев:

- события об изменении промежуточных состояний групповых задач и о применении политик занимают значительный процент всех событий в базе данных Kaspersky Security Center;
- в журнале событий Kaspersky Event Log появляются записи об автоматическом удалении событий при превышения заданного лимита на общее число событий, хранимых в базе данных.

Выберите параметры регистрации событий, исходя из того, что оптимальное количество событий, поступающих с одного устройства в день, не должно превышать 20 (см. раздел "Скорость заполнения событиями базы данных" на стр. 931). Вы можете немного увеличить максимальное количество событий, если это необходимо, но только в том случае, если количество устройств в вашей сети относительно невелико (менее 10 000).

Особенности и оптимальные параметры некоторых задач

Некоторые задачи имеют особенности, связанные с количеством устройств в сети. В этом разделе даны рекомендации по оптимальной настройке параметров для таких задач.

Обнаружение устройств, задача резервного копирования данных, задача обслуживания базы данных и групповые задачи обновления Kaspersky Endpoint Security входят в базовую функциональность Kaspersky Security Center.

Задача инвентаризации входит в возможность Системного администрирования и недоступна, если эта возможность не активирована.

В этом разделе

Частота обнаружения устройств

Не рекомендуется увеличивать установленную по умолчанию частоту поиска устройств, так как это может создать чрезмерную нагрузку на контроллеры домена. Рекомендуется, наоборот, устанавливать расписание опроса с минимально возможной частотой, насколько позволяют потребности вашей организации. В таблице ниже приведены рекомендации по расчету оптимального расписания.

Таблица 92. Расписание обнаружения устройств

Количество устройств в сети	Рекомендуемая частота для обнаружения устройств
Менее 10 000	Установленная по умолчанию или реже
10 000 и более	Один раз в сутки или реже

Задачи резервного копирования данных Сервера администрирования и обслуживания базы данных

Сервер администрирования перестает функционировать во время выполнения следующих задач:

- резервное копирование данных Сервера администрирования;
- Обслуживание базы данных.

Пока выполняются эти задачи, данные не могут поступать в базу данных.

Вам может потребоваться изменить расписание этих задач так, чтобы их выполнение не пересекалось по времени с выполнением других задач Сервера администрирования.

Групповые задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security версии 10 и выше рекомендуется расписание **При загрузке обновлений в хранилище** с установленным флажком **Автоматически определять интервал для распределения запуска**

задачи.

Если вы создали на каждой точке распространения локальную задачу загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security рекомендуется задать периодическое расписание. Значение периода автономизации в этом случае должно составлять один час.

Задача инвентаризации программного обеспечения

Количество исполняемых файлов, получаемых Сервером администрирования от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Количество файлов на обыкновенном управляемом устройстве, как правило, составляет не более 60 000. Количество исполняемых файлов на файловом сервере может быть больше и может даже превышать порог в 150 000.

Тестовые замеры показали, что на устройстве под управлением операционной системы Windows 7, на котором установлена программа Kaspersky Endpoint Security 11 и не установлены никакие сторонние программы, результаты выполнения задачи инвентаризации следующие:

- Когда флажки **Инвентаризация DLL-модулей** и **Инвентаризации файлов скриптов** сняты: около 3000 файлов.
- Когда флажки **Инвентаризация DLL-модулей** и **Инвентаризации файлов скриптов** установлены: от 10 000 до 20 000 файлов, в зависимости от количества установленных пакетов обновлений операционной системы.
- Когда установлен только флажок **Инвентаризации файлов скриптов**: приблизительно 10 000 файлов.

Информация о нагрузке на сеть между Сервером администрирования и защищаемыми устройствами

В этом разделе приводятся результаты тестовых замеров трафика в сети с указанием условий, при которых проводились замеры. Вы можете использовать эту информацию как справочную при планировании сетевой инфраструктуры и пропускной способности каналов внутри организации (либо между Сервером администрирования и организацией, в которой расположены защищаемые устройства). Зная пропускную способность сети, вы также можете приблизительно оценивать, сколько времени должна занять та или иная операция, связанная с передачей данных.

В этом разделе

Расход трафика при выполнении различных сценариев

В таблице ниже приводятся результаты тестовых замеров трафика между Сервером администрирования и управляемым устройством при выполнении различных сценариев.

Синхронизация устройства с Сервером администрирования происходит по умолчанию раз в 15 минут либо реже (см. раздел "Частота обнаружения устройств" на стр. 933). Однако если вы меняете на Сервере администрирования параметры политики или задачи, то происходит досрочная синхронизация устройств, для которых применима эта политика (задача), и новые параметры передаются на устройства.

Таблица 93. Трафик между Сервером администрирования и управляемым устройством

Сценарий	Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
Установка Kaspersky Endpoint Security 11 для Windows с обновленными базами	208 МБ	5,7 МБ
Установка Агента администрирования	40 МБ	1 ГБ
Совместная установка Агента администрирования и Kaspersky Endpoint Security 11 для Windows	248 МБ	6,3 МБ
Первоначальное обновление антивирусных баз без обновления баз в пакете (при отказе от участия в KSN)	160 КБ	5,5 МБ

Сценарий	Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
Ежесуточное обновление антивирусных баз; первоначальное обновление антивирусных баз (при участии в KSN)	32 КБ	5,3 МБ
Первоначальная синхронизация до обновления баз на устройстве (передача политик и задач)	254 КБ	221 КБ
Первоначальная синхронизация после обновления баз на устройстве	160 КБ	54 КБ
Синхронизация при отсутствии изменений на Сервере администрирования (по расписанию)	20 КБ	32 КБ
Синхронизация при изменении одного параметра в политике группы (досрочная, сразу после внесения изменения)	11 КБ	12 КБ
Синхронизация при изменении одного параметра в групповой задаче (досрочная, сразу после внесения изменения)	12 КБ	11 КБ
Принудительная синхронизация	7 КБ	11 КБ
Событие **Обнаружен вирус** (1 вирус)	28 КБ	42 КБ
Событие **Обнаружен вирус** (10 вирусов)	46 КБ	73 КБ

В таблице ниже представлен средний расход трафика за сутки между Сервером администрирования и управляемым устройством с установленным Агентом администрирования и Kaspersky Endpoint Security 11 для Windows при следующих условиях:

- Устройство не назначено точкой распространения.
- Системное администрирование не включено.
- Период синхронизации с Сервером администрирования составляет 15 минут.

Таблица 94. Средний расход трафика за сутки

Трафик от Сервера к управляемому устройству	Трафик от управляемого устройства к Серверу
52 МБ	4 МБ

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашего вопроса в документации или других источниках информации о программе, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки(https://support.kaspersky.com/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону(https://support.kaspersky.com/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount portal(https://companyaccount.kaspersky.com).

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.com/b2b).

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.com/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.com/faq/companyaccount_help).

Источники информации о программе

Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security Center (https://www.kaspersky.ru/small-to-medium-business-security/security-center), вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center в Базе знаний

База знаний – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Security Center в Базе знаний (https://support.kaspersky.ru/ksc11) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Security Center и с другими программами "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

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

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

Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 939).

Глоссарий

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Консоль администрирования

Компонент программы Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным сервисам Сервера администрирования и Агента администрирования.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Сервер администрирования может также управлять этими программами.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими устройствами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы "Лаборатории Касперского".

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего

восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Рабочее место администратора

Устройство, на котором установлена Консоль администрирования. Этот компонент, предоставляет интерфейс управления Kaspersky Security Center.

С рабочего места администратор управляет серверной частью Kaspersky Security Center. Используя рабочее место администратора, администратор выстраивает систему централизованной защиты сети организации, сформированной на базе программ "Лаборатории Касперского".

Инстанс Amazon EC2

Виртуальная машина, созданная на основе образа AMI с использованием Amazon Web Services.

Amazon Machine Image (AMI)

Шаблон с необходимой для запуска виртуальной машины конфигурацией программного обеспечения. На основе одного образа AMI можно создать несколько инстансов.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

Магазин приложений

Компонент программы Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать apk-файлы приложений и ссылки на приложения в Google Play.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Доступное обновление

Пакет обновлений модулей программы "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

AWS Application Program Interface (AWS API)

Программный интерфейс приложения платформы AWS, который используется программой Kaspersky Security Center. Средствами AWS API проводятся, в частности, опрос облачных сегментов и установка Агента администрирования на инстансы.

Ключ доступа AWS IAM

Комбинация, состоящая из ID ключа (вида "AKIAIOSFODNN7EXAMPLE") и секретного ключа (вида "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Пара принадлежит IAM-пользователю и используется для получения доступа к сервисам AWS.

Консоль управления AWS

Веб-интерфейс для просмотра и управления ресурсами в AWS. Консоль управления AWS доступна в интернете на странице https://aws.amazon.com/console/.

B

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Широковещательный домен

Логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещательного канала на уровне сетевой модели OSI (Open Systems Interconnection Basic

Reference Model).

C

Централизованное управление программой

Удаленное управление программой при помощи сервисов администрирования, предоставляемых Kaspersky Security Center.

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной безопасности организации-клиента.

Облачное окружение

Виртуальные машины на базе облачной платформы, объединенные в сети.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

D

Демилитаризованная зона (DMZ)

Демилитаризованная зона – это сегмент локальной сети, в которой находятся серверы, отвечающие на запросы из глобальной сети. В целях обеспечения безопасности локальной сети организации доступ в локальную сеть из демилитаризованной зоны ограничен и защищен сетевым экраном.

Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

Непосредственное управление программой

Управление программой через локальный интерфейс.

Точка распространения

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в составе группы администрирования и / или широковещательного домена. Точки распространения предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Точки распространения могут быть назначены автоматически Сервером администрирования или вручную администратором. Точка распространения ранее называлась агентом

обновлений.

E

EAS-устройство

Мобильное устройство, которое подключается к Серверу администрирования по протоколу Exchange ActiveSync. По протоколу Exchange ActiveSync могут подключаться и управляться устройства с операционными системами iOS, Android, Windows Phone®.

Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Ошибка.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Сервер Exchange

Компонент Kaspersky Security Center, который позволяет подключать мобильные устройства Exchange ActiveSync к Серверу администрирования. Устанавливается на клиентском устройстве.

F

Форсированная установка

Метод удаленной установки программ "Лаборатории Касперского", который позволяет провести удаленную установку программного обеспечения на конкретные клиентские устройства. Для успешного выполнения задачи методом форсированной установки учетная запись для запуска задачи должна обладать правами на удаленный запуск программ на клиентских устройствах. Данный метод рекомендуется для установки программ на устройства, работающие под управлением операционных систем Microsoft Windows NT / 2000 / 2003 / XP, в которых поддерживается такая возможность.

G

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

H

Домашний Сервер администрирования

Домашний Сервер администрирования – это Сервер администрирования, который был задан при установке Агента администрирования. Домашний Сервер администрирования может использоваться в параметрах профилей подключения Агента администрирования.

HTTPS

Безопасный протокол передачи данных между браузером и веб-сервером с использованием шифрования. HTTPS используется для доступа к закрытой информации, такой как корпоративные или финансовые данные.

I

IAM-роль

Совокупность прав для выполнения запросов к сервисам AWS. IAM-роли не связаны ни с каким конкретным пользователем или группой и обеспечивают права доступа без использования ключей доступа AWS IAM. IAM-роль можно присвоить пользователям IAM, инстансам EC2, приложениям или сервисам AWS.

IAM-пользователь

Пользователь сервисов AWS. IAM-пользователь может обладать правами на опрос облачного сегмента.

Identity and Access Management (IAM)

Сервис AWS, который позволяет управлять доступом пользователей к другим сервисам и ресурсам AWS.

Несовместимая программа

Антивирусная программа стороннего производителя или программа "Лаборатории Касперского", не поддерживающая управление через Kaspersky Security Center.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит

набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

Внутренние пользователи

Учетные записи внутренних пользователей используются для работы с виртуальными Серверами администрирования. В программе Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. Пользователь устанавливает iOS MDM-профиль на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

J

JavaScript

Язык программирования, расширяющий возможности веб-страниц. Веб-страницы, созданные с использованием JavaScript, способны выполнять дополнительные действия (например, изменять вид элементов интерфейса или открывать дополнительные окна) без обновления веб-страницы данными с веб-сервера. Чтобы просматривать веб-страницы, созданные с использованием JavaScript, в параметрах браузера надо включить поддержку JavaScript.

K

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории

Касперского" получают обновления баз и модулей программы.

Локальный KSN

Локальный Kaspersky Security Network – это решение, которое предоставляет пользователям устройств, с установленными программами "Лаборатории Касперского", доступ к базам данных Kaspersky Security Network и другим статистическим данным, без отправки данных со своих устройств в Kaspersky Security Network. Локальный Kaspersky Security предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

- Устройства пользователей не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

Kaspersky Security Center System Health Validator (SHV)

Компонент программы Kaspersky Security Center, предназначенный для проверки работоспособности операционной системы при совместной работе программы Kaspersky Security Center с Microsoft NAP.

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии. Вы можете использовать программу только при наличии файла ключа.

L

Срок действия лицензии

Период, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Группа лицензионных программ

Группа программ, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

Локальная установка

Установка программы безопасности на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива программы безопасности или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском компьютере.

M

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Плагин управления

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Он входит в состав всех программ "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky Security Center.

Ручная установка

Установка программы безопасности на устройство сети организации из дистрибутива программы безопасности. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

N

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft® Windows®. Для программ "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.

Антивирусная безопасность сети

Комплекс технических и организационных мер, снижающих вероятность проникновения на устройства сети организации вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании программ безопасности и сервисов, а также при наличии и соблюдении политики информационной безопасности в организации.

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных программ безопасности, использование ключей, количество и виды обнаруженных угроз.

P

Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.
- Средний.
- Низкий.

- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Профиль

Набор параметров поведения мобильных устройств Exchange при подключении к серверу Microsoft Exchange.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

R

Удаленная установка

Установка программ "Лаборатории Касперского" при помощи инструментов, предоставляемых программой Kaspersky Security Center.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами (на стр. 943).

S

Администратор поставщика услуг

Сотрудник организации-поставщика услуг антивирусной защиты. Выполняет работы по инсталляции, эксплуатации систем антивирусной защиты, созданных на основе решений "Лаборатории Касперского", а также осуществляет техническую поддержку клиентов.

Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

T

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

Параметры задачи

Параметры работы программы, специфичные для каждого типа задачи.

U

Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы безопасности.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

V

Виртуальный Сервер администрирования

Компонент программы Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования использует для работы базу данных главного Сервера администрирования: задачи резервного копирования и восстановления данных, проверки и получения обновлений не поддерживаются на виртуальном Сервере.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

W

Windows Server Update Services (WSUS)

Программа, которая используется для распространения обновлений программ Microsoft на устройствах пользователей в сети организации.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг IDC Worldwide Endpoint Security Revenue by Vendor). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух

лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	Https://virusdesk.kaspersky.ru (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SQL Server, OneNote, OutLook, Tahoma, Win32, Windows, Windows PowerShell, Windows Server, Windows Phone, Windows Vista, Windows Azure – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Adobe – товарный знак или зарегистрированный в США и/или других странах товарный знак Adobe Systems Incorporated.

AirPlay, AirDrop, AirPrint, App Store, Apple, AppleScript, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – товарные знаки Apple Inc., зарегистрированные в США и других странах.

AMD, AMD64 – товарные знаки Advanced Micro Devices, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Cisco, Cisco Systems, iOS – товарные знаки или зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Android, Chrome, Dalvik, Firebase, Google, Google Chrome, Google Play, Google Maps, Hangouts, YouTube – товарные знаки Google, Inc.

Mozilla Firefox – товарный знак Mozilla Foundation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Oracle, JavaScript, Python, TouchDown, Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

QRadar, IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Intel, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Parallels Desktop является зарегистрированным товарным знаком Parallels International GmbH в США и / или других странах.

SPL, Splunk – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

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.

VMware, VMware vSphere – товарные знаки или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 95. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
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

Указатель

A

E

I

K

R

S

A

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

Р