kaspersky

Kaspersky Security для виртуальных сред 6.0 Защита без агента

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.0

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 15.01.2020

Обозначение документа: 643.46856491.00098-02 90 01

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

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

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Security для виртуальных сред 6.0 Защита без агента" (далее также "Kaspersky Security", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Security, а также поддержка организаций, использующих Kaspersky Security. Документ адресован техническим специалистам, которые имеют опыт работы с виртуальной инфраструктурой на платформе VMware vSphere™ и системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

kaspersky

Источники информации о программе

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

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

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 173).

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

Страница Kaspersky Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security (http://www.kaspersky.ru/business-security/virtualization-agentless) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security в Базе знаний

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

На странице Kaspersky Security в Базе знаний (https://support.kaspersky.ru/ksv6nola) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Антивирусу Касперского, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входит контекстная справка и онлайн-справка (Online help). Контекстная справка содержит сведения о каждом окне плагина управления Kaspersky Security: перечень и описание параметров.

Онлайн-справка содержит информацию об установке, обновлении и удалении программы, об активации и подготовке программы к работе, о настройке параметров работы программы и об основных приемах работы с программой.

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

Сообщество пользователей "Лаборатории Касперского"

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

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

kaspersky

О программе

Программное изделие "Kaspersky Security для виртуальных сред 6.0 Защита без агента" (далее также "Kaspersky Security", "программа") представляет собой средство антивирусной защиты типов "Б" и "В" четвертого класса защиты и предназначено для применения на серверах и автоматизированных рабочих местах информационных систем.

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

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия.

В сертифицированной версии программы в виртуальной инфраструктуре не устанавливается компонент Защита от сетевых угроз.

kaspersky

Варианты использования программы

Защита виртуальной инфраструктуры под управлением одного или нескольких серверов VMware vCenter Server

SVM с компонентом Защита от файловых угроз разворачиваются на гипервизорах VMware ESXi™ под управлением одного или нескольких автономных серверов VMware vCenter Server® и обеспечивают защиту виртуальных машин, работающих на этих гипервизорах. Программа работает в обычном режиме.

Для управления программой требуется основной плагин управления Kaspersky Security. С помощью основного плагина управления вы можете настраивать индивидуальные параметры защиты виртуальной инфраструктуры под управлением каждого сервера VMware vCenter Server или общие параметры защиты всей виртуальной инфраструктуры.

Защита виртуальной инфраструктуры под управлением VMware vCloud Director

SVM с компонентом Защита от файловых угроз разворачиваются на гипервизорах VMware ESXi под управлением серверов VMware vCenter Server, подключенных к серверу VMware vCloud Director®. SVM могут защищать все виртуальные машины, работающие в виртуальной инфраструктуре, в том числе виртуальные машины, которые входят в организации vCloud Director.

Этот вариант использования программы позволяет обеспечить защиту изолированных виртуальных инфраструктур организаций-клиентов или подразделений одной организации (далее также "клиентов"). Программа работает в *режиме multitenancy*, то есть один экземпляр программы, установленный в инфраструктуре организации-провайдера антивирусной защиты (далее также "провайдера"), позволяет нескольким организациям-клиентам независимо управлять защитой своей виртуальной инфраструктуры.

Для управления программой требуется основной плагин управления Kaspersky Security и плагин управления для клиентов. Основной плагин управления позволяет настраивать общие параметры работы программы, а также параметры защиты от файловых угроз тех виртуальных машин, которые не входят в состав организаций vCloud Director, например виртуальных машин, принадлежащих провайдеру. Плагин управления для клиентов позволяет настраивать индивидуальные параметры защиты от файловых угроз для каждого клиента.

Для управления защитой клиентов используются виртуальные Серверы администрирования Kaspersky Security Center. Администратор провайдера создает для каждого клиента отдельный виртуальный Сервер администрирования и предоставляет администратору клиента доступ к нему. С помощью виртуального Сервера администрирования и плагина управления для клиентов администратор клиента может управлять защитой своей виртуальной инфраструктуры от файловых угроз (см. раздел "Инструкция по работе с программой для администратора организации-клиента" на стр. 136). Обновление баз программы, активацию программы и работу с копиями файлов, помещенных в резервное хранилище, обеспечивает провайдер.

Администратор провайдера может получать информацию о защищаемых виртуальных машинах клиентов с помощью отчета, который доступен на Сервере интеграции. По умолчанию ведение отчета выключено. О том, как включить запись информации в отчет и выгрузить отчет в файл в формате CSV, см. в Базе знаний http://support.kaspersky.ru/15307.

От выбранного варианта использования программы зависит порядок установки программы. Рекомендуется выбрать вариант использования программы перед началом установки. Если после установки программы в инфраструктуре под управлением одного или нескольких серверов VMware vCenter Server вы решили перейти к использованию программы в режиме multitenancy, чтобы обеспечить правильную работу программы, вам нужно выполнить дополнительные действия, описанные в Базе знаний http://support.kaspersky.ru/15319.

kaspersky

Требования

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

В этом разделе

Аппаратные и программные требования

Требования к компонентам Kaspersky Security Center

Для функционирования Kaspersky Security в локальной сети организации должна быть установлена программа Kaspersky Security Center одной из следующих версий:

- Kaspersky Security Center 11. Если установлена версия Kaspersky Security Center 11, программа Kaspersky Security может защищать виртуальную инфраструктуру под управлением VMware vCloud Director (в режиме multitenancy) или виртуальную инфраструктуру под управлением одного или нескольких серверов VMware vCenter Server (режим multitenancy не используется).
- Kaspersky Security Center 10 Service Pack 3. Если установлена версия Kaspersky Security Center 10 Service Pack 3, программа Kaspersky Security может защищать виртуальную инфраструктуру под управлением одного или нескольких серверов VMware vCenter Server (режим multitenancy не используется).

Если вы хотите использовать программу Kaspersky Security в режиме multitenancy, вам нужно установить Kaspersky Security Center 11.

Для работы программы требуются следующие компоненты Kaspersky Security Center:

- Сервер администрирования.
- Консоль администрирования.
- Агент администрирования. Этот компонент включен в состав образов SVM Kaspersky Security.

Сведения об установке Kaspersky Security Center см. в документации Kaspersky Security Center.

Операционная система на компьютере, где установлен Kaspersky Security Center, должна соответствовать требованиям компонента Сервер интеграции.

Программные требования компонента Сервер интеграции

Для установки и функционирования компонента Сервер интеграции на компьютере должна быть установлена одна из следующих операционных систем:

- Windows Server® 2019.

- Windows Server 2016.
- Windows Server 2012 R2 Datacenter / Standard / Essentials.

Для установки Сервера интеграции, Консоли Сервера интеграции и плагина управления Kaspersky Security требуется платформа Microsoft® .NET Framework 4.6.1.

Программные требования компонента Защита от файловых угроз

Для функционирования компонента Защита от файловых угроз виртуальная инфраструктура должна удовлетворять следующим программным требованиям:

- Вариант 1:
  - Гипервизор VMware ESXi 6.7 Update 3, гипервизор VMware ESXi 6.5 Update 3a или гипервизор VMware ESXi 6.0 Update 3a.
  - Сервер VMware vCenter Server 6.7 Update 3, сервер VMware vCenter Server 6.5 Update 3 или сервер VMware vCenter Server 6.0 Update 3j.
  - VMware NSX™ for vSphere™ 6.4.6.
- Вариант 2:
  - Гипервизор VMware ESXi 6.5 Update 3a или гипервизор VMware ESXi 6.0 Update 3a.
  - Сервер VMware vCenter Server 6.5 Update 3 или сервер VMware vCenter Server 6.0 Update 3j.
  - VMware NSX for vSphere 6.3.7.

Компонент Защита от файловых угроз обеспечивает защиту виртуальных машин, на которых установлены следующие гостевые операционные системы:

- Операционные системы Windows® для рабочих станций:
  - Windows 10.
  - Windows 8.1.
  - Windows 8.
  - Windows 7 Service Pack 1.
- Операционные системы Windows для серверов:
  - Windows Server 2019.
  - Windows Server 2016.
  - Windows Server 2012 R2 без поддержки ReFS (Resilient File System).
  - Windows Server 2012 без поддержки ReFS (Resilient File System).
  - Windows Server 2008 R2 Service Pack 1.

  На защищаемых виртуальных машинах с операционными системами Windows должна использоваться одна из следующих файловых систем: FAT, FAT32, NTFS, ISO9660, UDF, CIFS.
- Операционные системы Linux® для серверов:
  - Ubuntu Server 14.04 LTS (64-разрядная).
  - Red Hat Enterprise Linux® Server 7 GA (64-разрядная).
  - SUSE Linux Enterprise Server 12 GA (64-разрядная).
  - CentOS 7 (64-разрядная).

На защищаемых виртуальных машинах с операционными системами Linux должна использоваться одна из следующих файловых систем:

- локальные файловые системы: EXT2, EXT3, EXT4, XFS, BTRFS, VFAT, ISO9660;
- сетевые файловые системы: NFS, CIFS.

Для защиты виртуальных машин от файловых угроз на виртуальных машинах требуется установить драйвер Guest Introspection (NSX File Introspection Driver).

Для этого на виртуальных машинах с операционной системой Windows требуется установить пакет VMware Tools™ версии 11.0.1. При установке пакета VMware Tools нужно установить компонент NSX File Introspection Driver, который входит в состав пакета, по умолчанию компонент NSX File Introspection Driver не устанавливается.

Для установки компонента NSX File Introspection Driver на виртуальных машинах с операционной системой Linux предусмотрены специальные пакеты.

Информацию об установке и компонентов VMware™ см. в документации к продуктам VMware https://docs.vmware.com/.

Программные требования для работы программы в режиме multitenancy

Для функционирования программы в режиме multitenancy в виртуальной инфраструктуре должен быть установлен компонент VMware vCloud Director 9.7.0.3 for Service Providers.

Аппаратные требования

В зависимости от выбранной вами конфигурации SVM (виртуальная машина защиты) требуется следующее минимальное количество системных ресурсов:

Конфигурация	Количество процессоров	Объем выделенной оперативной памяти, ГБ	Объем выделенного свободного места на диске, ГБ
2 CPU 2 GB RAM	2	2	42
2 CPU 4 GB RAM	2	4	44
2 CPU 8 GB RAM	2	8	48
4 CPU 4 GB RAM	4	4	44
4 CPU 8 GB RAM	4	8	48

Для установки и функционирования Сервера интеграции компьютер должен удовлетворять следующим минимальным аппаратным требованиям:

- объем свободного места на диске – 3 ГБ;
- объем оперативной памяти:
  - для работы Консоли Сервера интеграции – 50 МБ;
  - для работы Сервера интеграции, который обслуживает не более 30 гипервизоров и 2000–2500 защищенных виртуальных машин – 300 МБ. Объем оперативной памяти может изменяться в зависимости от размера виртуальной инфраструктуры VMware.

Аппаратные требования Kaspersky Security Center см. в документации Kaspersky Security Center.

Аппаратные требования виртуальной инфраструктуры VMware см. в документации к продуктам VMware.

Аппаратные требования операционной системы Windows см. в документации к продуктам Windows.

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 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.

kaspersky

Концепция управления программой через Kaspersky Security Center

Управление программой Kaspersky Security для виртуальных сред 6.0 Защита без агента осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center. В случае программы Kaspersky Security для виртуальных сред 6.0 Защита без агента клиентским устройством Kaspersky Security Center является SVM. Защищенные виртуальные машины не являются клиентскими устройствами с точки зрения Kaspersky Security Center, так как на них не устанавливается Агент администрирования Kaspersky Security Center.

После установки Kaspersky Security в виртуальной инфраструктуре SVM передают информацию о себе в Kaspersky Security Center. На основании этой информации Kaspersky Security Center объединяет SVM в *кластеры KSC* (кластеры Kaspersky Security Center):

- Кластер "VMware vCenter Agentless" – кластер KSC, который соответствует автономному серверу VMware vCenter Server. Этот кластер содержит все SVM, развернутые на гипервизорах VMware ESXi под управлением одного автономного сервера VMware vCenter Server.

  Кластеру KSC, соответствующему серверу VMware vCenter Server, присваивается название *VMware vCenter '<имя>' (<IP-адрес или доменное имя>) Agentless*, где:

  - <имя> – имя сервера VMware vCenter Server, соответствующего этому кластеру KSC. Если имя VMware vCenter Server не задано или совпадает с его IP-адресом, то имя опускается.
  - <IP-адрес или доменное имя> – IP-адрес или доменное имя VMware vCenter Server, соответствующего этому кластеру KSC.

  Виртуальные машины, работающие под управлением этого сервера VMware vCenter Server, образуют *защищаемую инфраструктуру кластера "VMware vCenter Agentless"*.

- Кластер "VMware vCloud Director Agentless" – кластер KSC, который соответствует серверу VMware vCloud Director. Этот кластер содержит все SVM, развернутые на гипервизорах VMware ESXi под управлением всех серверов VMware vCenter Server, подключенных к одному VMware vCloud Director.

  Кластеру KSC, соответствующему серверу VMware vCloud Director, присваивается название *VMware vCloud Director (<IP-адрес или доменное имя>) Agentless*, где <IP-адрес или доменное имя> – IP-адрес или доменное имя VMware vCloud Director, соответствующего этому кластеру KSC.

  Виртуальные машины, работающие под управлением серверов VMware vCenter Server, подключенных к этому серверу VMware vCloudDirector, в том числе виртуальные машины в составе организаций vCloud Director, образуют защищаемую инфраструктуру кластера "VMware vCloud Director Agentless", соответствующего VMware vCloud Director.

Kaspersky Security Center создает в Консоли администрирования в папке **Управляемые устройства** для каждого кластера KSC отдельную группу администрирования и присваивает этой группе название кластера KSC. При выборе в дереве консоли группы администрирования с названием кластера KSC в рабочей области на закладке **Устройства** отображается список SVM, входящих в состав этого кластера KSC.

Управление работой программы Kaspersky Security через Kaspersky Security Center осуществляется с помощью политик и задач:

Политика – это набор параметров работы программы, заданный для группы администрирования. В случае программы Kaspersky Security политика применяется на SVM и определяет параметры, с которыми SVM защищают виртуальные машины, которые находятся в области действия политики (см. раздел "О политиках Kaspersky Security" на стр. 18).

Каждая политика содержит один или несколько профилей защиты. Профили защиты позволяют настроить параметры файловой защиты виртуальных машин.

> Термин "профиль защиты", используемый в этом документе, не следует путать с термином "профиль защиты" в нотации ГОСТ Р ИСО/МЭК 15408.

- *Задачи* выполняются на SVM и реализуют такие функции программы, как активация программы, проверка виртуальных машин, обновление баз программы.

Подробную информацию о политиках и задачах см. в документации Kaspersky Security Center.

В этом разделе

О политиках Kaspersky Security

При настройке параметров защиты виртуальной инфраструктуры рекомендуется учитывать особенности политик Kaspersky Security.

Область действия политики, то есть набор виртуальных машин, для защиты которых может использоваться политика, зависит от типа политики, защищаемой инфраструктуры, выбранной при настройке политики, и области применения политики (набора SVM, на которых применяется политика).

Типы политик Kaspersky Security

Для программы Kaspersky Security предусмотрены политики следующих типов:

- *Основная политика*. Позволяет настраивать параметры защиты виртуальных машин от файловых угроз с помощью профилей защиты (см. раздел "О профилях защиты Kaspersky Security" на стр. 20), а также следующие параметры работы программы:
  - параметры уведомлений о событиях в работе программы (см. раздел "Настройка параметров уведомлений о событиях" на стр. 134);
  - параметры резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 122);
  - параметры использования Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 129).

  Если программа работает в режиме multitenancy, основная политика определяет параметры защиты от файловых угроз для виртуальных машин, которые не входят в состав организаций vCloud Director.

Основные политики рекомендуется создавать на главном Сервере администрирования Kaspersky Security Center. Основные политики создаются с помощью основного плагина управления Kaspersky Security (см. раздел "Создание основной политики" на стр. 70).

- *Политика для клиентов* (используется, только если программа работает в режиме multitenancy). Позволяет настраивать параметры защиты для виртуальных машин, которые входят в состав организаций vCloud Director. С помощью этой политики вы можете задавать следующие параметры:
  - параметры уведомлений о событиях, произошедших во время защиты и проверки виртуальных машин клиента (только в политике, которая создана на главном Сервере администрирования Kaspersky Security Center);
  - индивидуальные параметры файловой защиты для виртуальных машин клиента;
  - параметры использования KSN для организации-клиента.

  Вы можете создавать политики для клиентов на главном или на виртуальных Серверах администрирования Kaspersky Security Center с помощью плагина управления Kaspersky Security для клиентов (см. раздел "Создание политики для клиентов" на стр. 73).

Защищаемая инфраструктура политики

В зависимости от защищаемой инфраструктуры, которую вы выбираете при настройке политики, различаются следующие политики:

- политика для одного сервера VMware vCenter Server – позволяет настраивать параметры защиты виртуальной инфраструктуры под управлением одного сервера VMware vCenter Server;
- политика для всей защищаемой инфраструктуры – позволяет настраивать параметры защиты виртуальной инфраструктуры под управлением всех серверов VMware vCenter Server, к которым подключается Сервер интеграции.

Область применения политики

В случае программы Kaspersky Security политика применяется на SVM. Каждая SVM может защищать только виртуальные машины, работающие на том гипервизоре, на котором развернута SVM. Поэтому область действия политики (набор виртуальных машин, для защиты которых может использоваться политика) зависит от области применения политики (набора SVM, на которых применяется политика).

Область применения политики определяется расположением политики в иерархии групп администрирования Kaspersky Security Center. Политика применяется на SVM следующим образом:

- основная политика в группе администрирования, содержащей кластер KSC, применяется на всех SVM этого кластера KSC;
- основная политика в группе администрирования или папке, которая является родительской по отношению к группам, содержащим кластеры KSC, применяется на всех SVM дочерних кластеров KSC;
- политика для клиентов на виртуальном Сервере администрирования, созданном в группе кластера "VMware vCloud Director Agentless", соответствующего VMware vCloud Director, применяется на всех SVM этого кластера KSC.

Наследование параметров политик

В соответствии с порядком наследования политик Kaspersky Security Center параметры политик по умолчанию передаются в политики вложенных групп администрирования и подчиненных Серверов администрирования (см. подробнее в документации Kaspersky Security Center). Параметры и блоки параметров политик имеют *атрибут "замок"*, который показывает, наложен ли запрет на изменение этих параметров в политиках вложенного уровня иерархии. Если в политике для параметра или блока параметров "замок" закрыт (),

значения этих параметров записываются в политиках вложенного уровня иерархии и переопределить эти значения невозможно.

О профилях защиты Kaspersky Security

Термин "профиль защиты", используемый в этом документе, не следует путать с термином "профиль защиты" в нотации ГОСТ Р ИСО/МЭК 15408.

В политиках Kaspersky Security предусмотрены следующие профили защиты:

- *Основной профиль защиты* автоматически формируется во время создания политики. Основной профиль защиты недоступен для удаления, однако вы можете изменять значения параметров основного профиля защиты.
- *Дополнительные профили защиты* вы можете создать после создания политики. Благодаря дополнительным профилям защиты вы можете гибко настраивать разные параметры защиты для разных виртуальных машин в составе защищаемой инфраструктуры. Политика может содержать несколько дополнительных профилей защиты.

В профилях защиты вы можете настраивать следующие параметры защиты от файловых угроз (см. раздел «Защита виртуальных машин от файловых угроз» на стр. 83):

- Уровень безопасности. Вы можете выбрать один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**) или настроить уровень безопасности самостоятельно (**Пользовательский**). Уровень безопасности определяет следующие параметры проверки:
  - проверка архивов, самораспаковывающихся архивов, вложенных OLE-объектов, составных файлов;
  - ограничение проверки файлов по времени;
  - список объектов для обнаружения.
- Действие, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы.
- Область защиты (проверка сетевых дисков во время защиты виртуальных машин).
- Исключения из защиты (по имени, расширению или полному пути к файлу, по маске файла или по пути к папке, файлы которой не надо проверять).

Профиль защиты может быть назначен отдельному объекту виртуальной инфраструктуры VMware или корневому элементу защищаемой инфраструктуры, в роли которого может выступать, например, Сервер интеграции (см. рис. ниже).

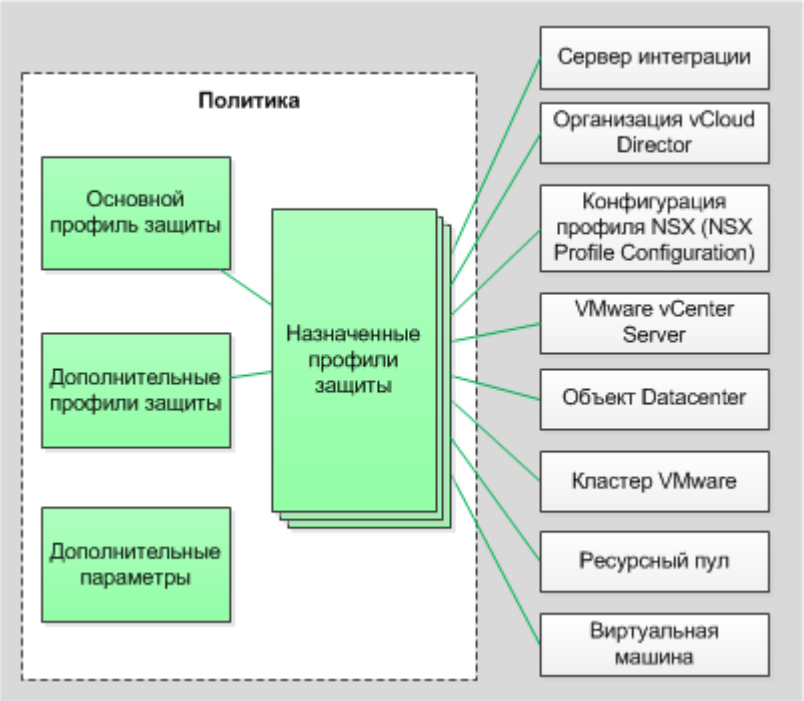

Рисунок 1. Профили защиты

Профиль защиты, назначенный корневому элементу защищаемой инфраструктуры, по умолчанию наследуется всеми дочерними элементами защищаемой инфраструктуры (например, всеми серверами VMware vCenter Server, к которым подключается Сервер интеграции). Профили защиты наследуются также согласно иерархии объектов виртуальной инфраструктуры VMware: профиль защиты, назначенный объекту виртуальной инфраструктуры, по умолчанию наследуется всеми его дочерними объектами, в том числе и виртуальными машинами. Вы можете назначить виртуальной машине собственный профиль защиты (см. раздел «Назначение профилей защиты объектам виртуальной инфраструктуры» на стр. 96) или использовать для нее профиль защиты, унаследованный от родительского объекта.

В основной политике, которая определяет параметры защиты виртуальной инфраструктуры под управлением одного сервера VMware vCenter Server, вы можете непосредственно назначать профили защиты объектам виртуальной инфраструктуры или использовать конфигурации профилей NSX (NSX Profile Configurations) для назначения параметров файловой защиты (см. раздел "Назначение профилей защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)" на стр. 97).

Одному объекту виртуальной инфраструктуры может быть назначен только один профиль защиты. Kaspersky Security защищает виртуальные машины с теми параметрами, которые указаны в назначенном этим виртуальным машинам профиле защиты.

Объекты виртуальной инфраструктуры, которым не назначен профиль защиты, исключаются из защиты.

Если вы исключаете объект виртуальной инфраструктуры из защиты, то по умолчанию из защиты исключаются также все дочерние объекты. Вы можете указать, следует ли исключать из защиты дочерние объекты, которым назначен собственный профиль защиты.

Наследование профилей защиты позволяет назначать одинаковые параметры защиты или исключать из защиты несколько виртуальных машин одновременно. Например, вы можете назначить одинаковые профили защиты виртуальным машинам в составе кластера VMware или ресурсного пула.

kaspersky

Об управлении политиками

Политики создаются с помощью мастера, который запускается по кнопке **Новая политика**, расположенной в рабочей области папки или группы администрирования на закладке **Политики**.

В папке или группе администрирования можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

Вы можете изменять параметры политики после ее создания в окне свойств политики.

► *Чтобы открыть окно свойств политики, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
2. В рабочей области выберите закладку **Политики**.
3. В списке политик выберите политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши по политике или выбрав в контекстном меню пункт **Свойства**.

Вы также можете выполнять следующие действия с политиками:

- копировать политики из одной папки или группы администрирования в другую;
- экспортировать политики в файл и импортировать политики из файла;
- конвертировать политики предыдущей версии программы;
- удалять политики.

Подробнее об управлении политиками см. в документации Kaspersky Security Center.

Особенности использования политик Kaspersky Security

Основная политика в папке Управляемые устройства **главного Сервера администрирования**

Такая политика автоматически создается с помощью мастера первоначальной настройки управляемой программы после установки основного плагина управления Kaspersky Security (см. раздел "Политики и задачи по умолчанию" на стр. 45). Вы также можете создать такую политику вручную с помощью мастера создания политики.

Политика применяется на всех SVM всех кластеров KSC.

В качестве защищаемой инфраструктуры для этой политики требуется выбрать всю защищаемую инфраструктуру. В роли корневого элемента защищаемой инфраструктуры выступает Сервер интеграции.

Параметры файловой защиты, настроенные в этой политике, распространяются на все виртуальные машины в составе защищаемой инфраструктуры политики, кроме виртуальных машин, которые входят в состав организаций vCloud Director.

Файловая защита по умолчанию выключена.

Чтобы включить файловую защиту, вам нужно назначить профили защиты объектам защищаемой инфраструктуры в свойствах политики (см. раздел "Назначение профилей защиты объектам виртуальной

инфраструктуры" на стр. 96). Вы можете назначить автоматически созданный основной профиль защиты или создать и назначить дополнительные профили защиты.

Рекомендуется учитывать, что параметры основной политики, расположенной в папке **Управляемые устройства**, наследуются основными политиками, расположенными во всех вложенных группах администрирования. Параметры, которые закрыты "замком", невозможно переопределить в политиках вложенного уровня иерархии.

Основная политика, размещенная в группе, которая содержит кластер "VMware vCenter Agentless"

Вы можете создать такую политику вручную с помощью мастера создания политики. Политика применяется на всех SVM этого кластера "VMware vCenter Agentless".

В качестве защищаемой инфраструктуры для этой политики требуется выбрать один сервер VMware vCenter Server и указать VMware vCenter Server, соответствующий кластеру "VMware vCenter Agentless". Корневой элемент защищаемой инфраструктуры – указанный VMware vCenter Server.

В области действия этой политики находятся все виртуальные машины в составе защищаемой инфраструктуры этого кластера "VMware vCenter Agentless".

Файловая защита включена по умолчанию: основной профиль защиты назначен серверу VMware vCenter Server и наследуется всеми дочерними объектами виртуальной инфраструктуры. Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе защищаемой инфраструктуры этого кластера KSC, вам нужно создать и назначить дополнительные профили защиты в свойствах политики.

Основная политика, размещенная в группе, которая содержит кластер "VMware vCloud Director Agentless"

Вы можете создать такую политику вручную с помощью мастера создания политики. Политика применяется на всех SVM этого кластера "VMware vCloud Director Agentless".

В качестве защищаемой инфраструктуры для этой политики требуется выбрать всю защищаемую инфраструктуру. В роли корневого элемента защищаемой инфраструктуры выступает Сервер интеграции.

Параметры файловой защиты, настроенные в этой политике, распространяются на все виртуальные машины в составе защищаемой инфраструктуры кластера "VMware vCloud Director Agentless", которые не входят в состав организаций vCloud Director.

Файловая защита по умолчанию выключена.

Чтобы включить файловую защиту, вам нужно назначить профили защиты объектам защищаемой инфраструктуры в свойствах политики. Вы можете назначить автоматически созданный основной профиль защиты или создать и назначить дополнительные профили защиты.

В свойствах основной политики для кластера "VMware vCloud Director Agentless" вы можете назначать профили защиты любым объектам защищаемой инфраструктуры. Но параметры файловой защиты будут применяться только для защиты виртуальных машин, которые не входят в состав организаций vCloud Director и находятся под управлением серверов VMware vCenter Server, подключенных к VMware vCloud Director, которому соответствует кластер "VMware vCloud Director Agentless".

Политика для клиентов в папке Управляемые устройства **главного Сервера администрирования**

Такая политика автоматически создается с помощью мастера первоначальной настройки управляемой программы после установки плагина управления Kaspersky Security для клиентов на главном Сервере

администрирования (см. раздел "Политики и задачи по умолчанию" на стр. 45). Вы также можете создать такую политику вручную с помощью мастера создания политики.

Если в папке **Управляемые устройства** главного Сервера администрирования отсутствует политика для клиентов, в Kaspersky Security Center не регистрируются события, которые произошли во время проверки и защиты виртуальных машин клиентов.

Параметры этой политики не используются непосредственно для защиты виртуальных машин: защищаемая инфраструктура для этой политики не выбирается. Но параметры основного профиля защиты и параметры использования KSN, настроенные в этой политике, могут наследоваться в политиках для клиентов, расположенных во вложенных группах администрирования, например, в папке **Управляемые устройства** виртуального Сервера администрирования. Таким образом, вы можете задавать единые параметры файловой защиты для виртуальных инфраструктур всех клиентов.

В этой политике вы можете настраивать параметры уведомлений о событиях, произошедших во время защиты и проверки виртуальных машин клиентов.

Рекомендуется учитывать, что параметры, которые закрыты "замком" в политике для клиентов на главном Сервере администрирования, будут недоступны для изменения на виртуальных Серверах администрирования. Администраторы клиентов не смогут настраивать эти параметры.

Политика для клиентов, размещенная в группе, содержащей кластер "VMware vCloud Director Agentless"

Эта политика аналогична политике для клиентов в папке **Управляемые устройства** главного Сервера администрирования (см. выше). Вы можете создать такую политику вручную с помощью мастера создания политики.

Политика для клиентов в папке Управляемые устройства **виртуального Сервера администрирования**

Вы можете создать такую политику вручную с помощью мастера создания политики.

Политика применяется на всех SVM кластера "VMware vCloud Director Agentless", соответствующего VMware vCloud Director, к которому относится организация vCloud Director, содержащая виртуальные машины клиента.

Защищаемая инфраструктура для этой политики выбирается автоматически. Корневым объектом является условный объект "Организация vCloud Director", который объединяет все виртуальные Datacenter клиента.

В области действия этой политики находятся все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования.

Файловая защита включена по умолчанию: основной профиль защиты назначен корневому объекту "Организация vCloud Director" и наследуется всеми объектами виртуальной инфраструктуры клиента. Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе виртуальной инфраструктуры клиента, вам нужно создать и назначить дополнительные профили защиты в свойствах политики.

О задачах Kaspersky Security

Для управления программой Kaspersky Security через Kaspersky Security Center рекомендуется использовать задачи следующих типов:

- *Групповая задача* – задача, которая выполняется на клиентских устройствах выбранной группы администрирования. Применительно к программе Kaspersky Security групповые задачи могут выполняться на SVM одного кластера KSC или на всех SVM.
- *Глобальная задача* – задача для одной или нескольких SVM, независимо от их нахождения в группе администрирования.

Подробнее о работе с задачами см. в документации Kaspersky Security Center.

Для Kaspersky Security предусмотрены следующие задачи:

- задачи полной и выборочной проверки, которые позволяют выполнять проверку всех или только указанных виртуальных машин, находящихся в области действия задачи;
- служебные задачи, которые позволяют активировать программу, обновлять базы программы и откатывать обновления.

Задачи создаются с помощью мастера, который запускается по кнопке **Новая задача**, расположенной в рабочей области папки или группы администрирования на закладке **Задачи**.

Вы можете изменять параметры задачи после ее создания в окне свойств задачи.

► *Чтобы открыть окно свойств задачи, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана задача.
2. В рабочей области выберите закладку **Задачи**.
3. В списке задач выберите задачу и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши по задаче или выбрав в контекстном меню пункт **Свойства**.

Вне зависимости от выбранного режима запуска задачи вы можете запускать и останавливать задачи в любой момент.

► *Чтобы запустить или остановить задачу, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана задача.
2. В рабочей области выберите закладку **Задачи**.
3. В списке задач выберите задачу, которую вы хотите запустить или остановить.
4. Нажмите на кнопку **Запустить** или на кнопку **Остановить**. Кнопки расположены справа от списка задач.

Информацию о ходе и результатах выполнения задач вы можете посмотреть в Консоли администрирования Kaspersky Security Center одним из следующих способов:

- В окне **Результаты выполнения задачи**. Окно открывается по ссылке **Просмотреть результаты**, расположенной справа от списка задач, который отображается в папке **Задачи** дерева консоли Kaspersky Security Center или на закладке **Задачи** в рабочей области папки или группы администрирования.
- В списке событий, которые SVM отправляют на Сервер администрирования Kaspersky Security Center. Список событий отображается на закладке **События** в рабочей области узла **Сервер администрирования**.

Вы также можете выполнять следующие действия с задачами:

- копировать задачи из одной папки или группы администрирования в другую;
- экспортировать задачи в файл и импортировать задачи из файла;
- конвертировать задачи предыдущей версии программы;
- удалять задачи.

Подробнее об управлении задачами см. в документации Kaspersky Security Center.

Задачи проверки

Задача полной проверки позволяет выполнять антивирусную проверку файлов всех виртуальных машин, находящихся в области действия задачи.

Задача выборочной проверки позволяет выполнять антивирусную проверку файлов указанных виртуальных машин из области действия задачи.

Область действия задач проверки зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

Вы можете создавать задачи проверки с помощью одного из плагинов управления Kaspersky Security:

- с помощью основного плагина управления – для проверки виртуальных машин, которые не входят в организации vCloud Director;
- с помощью плагина управления для клиентов – для проверки виртуальных машин, которые входят в организации vCloud Director, то есть для проверки виртуальных машин клиентов.

Задача полной проверки, созданная с помощью основного плагина управления

Если вы создаете задачу полной проверки с помощью основного плагина управления Kaspersky Security, область действия задачи определяется следующим образом:

- задача в папке **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center позволяет проверять все виртуальные машины в составе всей защищаемой инфраструктуры, которые не входят в организации vCloud Director;
- задача в группе, которая содержит кластер KSC, позволяет проверять все виртуальные машины в составе защищаемой инфраструктуры этого кластера KSC, не входящие в организации vCloud Director;
- задача в папке **Задачи**, настроенная для одной или нескольких SVM, позволяет проверять все виртуальные машины, находящиеся под защитой указанных SVM и не входящие в организации vCloud Director.

  SVM может проверять только виртуальные машины, работающие на том гипервизоре, на котором развернута SVM.

Задача полной проверки, созданная с помощью плагина управления для клиентов

Создание задачи полной проверки для виртуальных машин клиентов поддерживается только на виртуальном Сервере администрирования Kaspersky Security Center. Вы можете создать задачу полной проверки с помощью плагина управления Kaspersky Security для клиентов в папке **Управляемые устройства**

виртуального Сервера администрирования. В области действия этой задачи находятся все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования.

Задача выборочной проверки, созданная с помощью основного плагина управления

Задача выборочной проверки, созданная с помощью основного плагина управления, позволяет проверять виртуальные машины, которые находятся под управлением одного сервера VMware vCenter Server и не входят в организации vCloud Director.

Рекомендуется создавать задачи выборочной проверки с помощью основного плагина управления в следующих группах администрирования:

- если вы хотите проверять виртуальные машины под управлением автономного сервера VMware vCenter Server, вам нужно создать задачу в группе, которая содержит кластер "VMware vCenter Agentless", соответствующий этому VMware vCenter Server и указать в качестве области действия задачи этот сервер VMware vCenter Server.
- если вы хотите проверять виртуальные машины под управлением сервера VMware vCenter Server, подключенного к VMware vCloud Director, вам нужно создать задачу в группе, которая содержит кластер "VMware vCloud Director Agentless", соответствующий VMware vCloud Director, и указать в качестве области действия задачи нужный сервер VMware vCenter Server. Для каждого сервера VMware vCenter Server, подключенного к VMware vCloud Director, вам нужно создать отдельную задачу выборочной проверки.

В рамках выбранной области действия вам нужно указать виртуальные машины, которые требуется проверять. Вы можете указывать отдельные виртуальные машины, объекты виртуальной инфраструктуры VMware более высокого уровня иерархии или группы безопасности NSX (NSX Security Group), в которые входят нужные виртуальные машины.

В связи с особенностями настройки области действия задачи выборочной проверки рекомендуется создавать задачи выборочной проверки только в указанных группах администрирования, то есть групповые задачи. Если задача выборочной проверки настроена для одной или нескольких SVM (то есть является локальной или глобальной задачей), не гарантируется возможность правильной настройки области действия задачи.

Задача выборочной проверки, созданная с помощью плагина управления для клиентов

Создание задачи выборочной проверки для виртуальных машин клиентов поддерживается только на виртуальном Сервере администрирования Kaspersky Security Center. Вы можете создать задачу выборочной проверки с помощью плагина управления Kaspersky Security для клиентов в папке **Управляемые устройства** виртуального Сервера администрирования. В области действия этой задачи находятся все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования. В рамках этой области действия вам нужно указать виртуальные машины, которые требуется проверять. Вы можете указывать отдельные виртуальные машины или объекты виртуальной инфраструктуры VMware более высокого уровня иерархии.

Служебные задачи

Для управления программой вы можете использовать следующие служебные задачи:

- **Обновление**. В результате выполнения задачи устанавливаются обновления баз программы на SVM, на которых выполнялась задача.

- **Откат обновления**. В результате выполнения задачи происходит откат последнего обновления баз программы на SVM, на которых выполнялась задача.
- **Активация программы**. В результате выполнения задачи лицензионный ключ для активации программы или для продления срока действия лицензии добавляется на SVM, на которых выполнялась задача.

Вы можете создавать служебные задачи с помощью основного плагина управления Kaspersky Security на главном Сервере администрирования.

Набор SVM, на которых выполняются служебные задачи, зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center:

- задача в папке **Управляемые устройства** выполняется на всех SVM;
- задача в группе, которая содержит кластер KSC, выполняется на всех SVM одного кластера KSC;
- задача в папке **Задачи**, настроенная для одной или нескольких SVM, выполняется на указанных SVM.

О Сервере интеграции

Сервер интеграции – это компонент программы Kaspersky Security, осуществляющий взаимодействие между компонентами программы Kaspersky Security и виртуальной инфраструктурой VMware.

Сервер интеграции используется для выполнения следующих задач:

- Регистрация в VMware NSX Manager™ службы защиты файловой системы Kaspersky Security (Kaspersky File Antimalware Protection). Служба Kaspersky File Antimalware Protection необходима для установки компонента Защита от файловых угроз в инфраструктуре VMware.

  Ввод параметров, необходимых для регистрации и развертывания службы Kaspersky File Antimalware Protection, выполняется с помощью мастера, который запускается из Консоли Сервера интеграции (см. раздел "О Консоли Сервера интеграции" на стр. 29).
- Настройка конфигурации новых SVM и изменение конфигурации ранее развернутых SVM. Сервер интеграции передает на SVM параметры, которые вы задали в Консоли Сервера интеграции.
- Получение от сервера VMware vCenter Server и передача компонентам программы информации о виртуальной инфраструктуре (о гипервизорах и виртуальных машинах, работающих на каждом гипервизоре). Плагин управления Kaspersky Security и SVM в ходе своей работы обращаются к Серверу интеграции для получения информации о виртуальной инфраструктуре.
- Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center. Если вы используете программу Kaspersky Security в режиме multitenancy, для защиты виртуальной инфраструктуры каждой организации-клиента требуется установить соответствие между организацией vCloud Director, которая содержит виртуальные машины клиента, и виртуальным Сервером администрирования. Настройка списка соответствий выполняется в Консоли Сервера интеграции.

Во время работы Сервер интеграции сохраняет следующую информацию:

- параметры подключения к Серверу интеграции, в том числе пароли учетных записей Сервера интеграции;
- параметры подключения Сервера интеграции к VMware vCenter Server, VMware vCloud Director и VMware NSX Manager;

- параметры конфигурации SVM, в том числе пароли учетных записей root и klconfig, используемые на SVM;
- список защищаемых виртуальных машин с указанием времени последних событий, произошедших в ходе защиты и проверки объектов файловой системы.

Все данные, кроме списка защищаемых виртуальных машин, хранятся в защищенном виде. Информация сохраняется на компьютере, на котором установлен Сервер интеграции, и не отправляется в "Лабораторию Касперского".

О Консоли Сервера интеграции

Консоль Сервера интеграции содержит следующие разделы:

Раздел Параметры Сервера интеграции

В этом разделе вы можете посмотреть информацию о Сервере интеграции.

Раздел Учетные записи Сервера интеграции

В этом разделе вы можете изменить пароли учетных записей, которые используются для подключения к Серверу интеграции.

Раздел Защита виртуальной инфраструктуры

Этот раздел открывается по умолчанию после запуска Консоли Сервера интеграции. В этом разделе вы можете настроить подключение Сервера интеграции к серверам управления виртуальной инфраструктурой (VMware vCenter Server и VMware vCloud Director), задать или изменить параметры регистрации и развертывания служб Kaspersky Security, отменить регистрацию служб Kaspersky Security.

В таблице отображаются все серверы управления виртуальной инфраструктурой (VMware vCenter Server и VMware vCloud Director), к которым настроено подключение для Сервера интеграции (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49).

Над таблицей расположены следующие кнопки:

- Кнопка **Добавить** открывает окно **Подключение к виртуальной инфраструктуре**. В этом окне вы можете выбрать тип сервера управления виртуальной инфраструктурой, к которому требуется настроить подключение, и ввести параметры подключения к серверу VMware vCenter Server или VMware vCloud Director: IP-адрес в формате IPv4 или полное доменное имя (FQDN), имя и пароль учетной записи, под которой Сервер интеграции подключается к серверу.
- Кнопка **Обновить** позволяет обновить статус взаимодействия Сервера интеграции с виртуальной инфраструктурой.

Для каждого сервера VMware vCenter Server в таблице отображается следующая информация:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера VMware vCenter Server.
- Блок параметров, который содержит сообщения об ошибках подключения (если они есть) и список действий, которые вы можете выполнить при настройке подключения к этому VMware vCenter Server и для дальнейшего развертывания защиты виртуальной инфраструктуры под управлением этого VMware vCenter Server. Вы можете развернуть или свернуть список возможных действий для каждого сервера VMware vCenter Server щелчком левой клавиши мыши по адресу или имени сервера.
- Информация о развертывании защиты на кластерах VMware под управлением этого сервера VMware vCenter Server в виде *N/M*, где:

- N – количество гипервизоров VMware ESXi, на которых развернута служба защиты файловой системы (Kaspersky File Antimalware Protection), или прочерк, если служба не зарегистрирована в VMware NSX Manager;
- M – количество гипервизоров VMware ESXi, на которых развернута служба сетевой защиты (Kaspersky Network Protection), или прочерк, если служба не зарегистрирована в VMware NSX Manager.

  Возможность установки компонента Защита от сетевых угроз не предусмотрена для сертифицированной конфигурации программы.

  В скобках указывается общее количество гипервизоров VMware ESXi под управлением этого сервера VMware vCenter Server.

Для каждого сервера VMware vCloud Director в таблице отображается следующая информация:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера VMware vCloud Director.
- Блок параметров, который содержит сообщения об ошибках подключения (если они есть) и список действий, которые вы можете выполнить при настройке подключения к этому VMware vCloud Director и для дальнейшего развертывания защиты виртуальной инфраструктуры под управлением этого VMware vCloud Director. Вы можете развернуть или свернуть список возможных действий для каждого сервера VMware vCloud Director щелчком левой клавиши мыши по адресу или имени сервера.

Если не удалось установить соединение с VMware vCenter Server, VMware vCloud Director или с VMware NSX Manager, в таблице отображается предупреждение.

Если ошибка подключения происходит потому, что сертификат, полученный от VMware vCenter Server, VMware vCloud Director или от VMware NSX Manager, не является доверенным для Сервера интеграции, но полученный сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и установить подключение. Для этого по ссылке в описании проблемы нужно открыть окно **Подтверждение сертификата** и нажать на кнопку **Установить сертификат**. Полученный сертификат сохраняется в качестве доверенного для Сервера интеграции.

Доверенными для Сервера интеграции считаются также сертификаты, которые являются доверенными в операционной системе, в которой установлен Сервер интеграции.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Список возможных действий для VMware vCenter Server:

- **Зарегистрировать службы Kaspersky Security** – запускает мастер, с помощью которого вы можете ввести параметры, необходимые для регистрации в VMware NSX Manager и развертывания службы защиты файловой системы (Kaspersky File Antimalware Protection) на кластерах VMware, а также для настройки конфигурации новых SVM (см. раздел "Регистрация службы Kaspersky File Antimalware Protection" на стр. 51). По окончании ввода параметров Сервер интеграции выполняет регистрацию службы Kaspersky File Antimalware Protection в VMware NSX Manager.
- **Изменить параметры Kaspersky Security** – запускает мастер, с помощью которого вы можете изменить параметры подключений для взаимодействия Сервера интеграции с VMware NSX Manager, указать или изменить образ SVM для службы защиты файловой системы (Kaspersky File Antimalware

Protection), а также изменить параметры конфигурации SVM, которые применяются на новых SVM и на ранее развернутых SVM. По окончании ввода параметров Сервер интеграции применяет новые параметры и, если требуется, выполняет повторную регистрацию службы Kaspersky Security в VMware NSX Manager.

- **Отменить регистрацию служб Kaspersky Security** – открывает окно, в котором вы можете указать службу Kaspersky Security, регистрацию которой в VMware NSX Manager требуется отменить. Отмену регистрации выполняет Сервер интеграции.

  Отмена регистрации службы Kaspersky Security возможна, только если на кластерах VMware удалены все SVM и служба не используется в политиках безопасности NSX (NSX Security Policy). Удаление SVM и настройка политик безопасности NSX выполняется в консоли VMware vSphere™ Web Client.

- **Изменить параметры подключения к VMware vCenter Server** – открывает окно **Подключение к виртуальной инфраструктуре**, в котором вы можете изменить параметры подключения Сервера интеграции к VMware vCenter Server (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49).

- **Удалить VMware vCenter Server из списка** – открывает окно, в котором вы можете подтвердить удаление параметров подключения Сервера интеграции к этому VMware vCenter Server (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49). Сервер VMware vCenter Server будет удален из списка серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

  Удаление сервера VMware vCenter Server из списка возможно, только если служба Kaspersky Security не зарегистрирована в VMware NSX Manager.

Список возможных действий для VMware vCloud Director:

- **Установить соответствия для организаций vCloud Director** – открывает окно **Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования**, в котором вы можете установить соответствие между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования Kaspersky Security Center (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).

- **Изменить параметры подключения к VMware vCloud Director** – открывает окно **Подключение к виртуальной инфраструктуре**, в котором вы можете изменить параметры подключения Сервера интеграции к VMware vCloud Director (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49).

- **Удалить VMware vCloud Director из списка** – открывает окно, в котором вы можете подтвердить удаление параметров подключения Сервера интеграции к этому VMware vCloud Director (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49). Сервер VMware vCloud Director будет удален из списка серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

Раздел Управление защитой организаций-клиентов

Этот раздел используется, только если программа работает в режиме multitenancy.

В этом разделе вы можете выполнить следующие действия:

- Подключить Сервер интеграции к Серверу администрирования Kaspersky Security Center (см. раздел "Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 60).

  Сервер интеграции подключается к Серверу администрирования Kaspersky Security Center, чтобы получить информацию о виртуальных Серверах администрирования, созданных в Kaspersky Security Center, и установить соответствие между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования.

- Посмотреть или настроить список соответствий между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования Kaspersky Security Center (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).

  Настройка соответствия между организацией vCloud Director и виртуальным Сервером администрирования требуется, чтобы защищать виртуальные машины, которые входят в эту организацию vCloud Director, с помощью программы Kaspersky Security.

kaspersky

Подготовка к установке программы

Перед началом установки компонентов Kaspersky Security вам нужно выполнить следующие действия:

- Проверить соответствие компонентов Kaspersky Security Center и компонентов VMware программным требованиям для установки Kaspersky Security (см. раздел "Аппаратные и программные требования" на стр. 13).
- Подготовить образ SVM с компонентом Защита от файловых угроз (см. раздел "Подготовка образа SVM" на стр. 37).
- Разместить все файлы образов SVM в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS. Например, вы можете опубликовать образы SVM на Веб-сервере Kaspersky Security Center (см. подробнее в документации Kaspersky Security Center).
- Подготовить виртуальную инфраструктуру VMware к установке программы (см. раздел "Подготовка виртуальной инфраструктуры VMware" на стр. 33).
- В настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика, открыть порты, которые требуются для установки и работы компонентов программы (см. раздел "Используемые порты" на стр. 36).
- Настроить параметры учетных записей, которые требуются для установки и работы программы (см. раздел "Учетные записи для установки и работы программы" на стр. 34).

В этом разделе

Подготовка виртуальной инфраструктуры VMware

Перед установкой программы в виртуальной инфраструктуре VMware требуется выполнить следующие действия:

- Объединить гипервизоры VMware ESXi в один или несколько кластеров VMware.
- Настроить в свойствах каждого гипервизора параметры **Agent VM Settings**: выбрать сеть и хранилище для служебных виртуальных машин и SVM. Подробнее о настройке параметров **Agent VM Settings** см. в документации к продуктам VMware https://docs.vmware.com/.
- На каждом кластере VMware развернуть службу Guest Introspection (см. раздел "Развертывание службы Guest Introspection" на стр. 34).
- Установить драйвер Guest Introspection (NSX File Introspection Driver) на каждой виртуальной машине, которую вы хотите защищать с помощью Kaspersky Security.

  Для этого на виртуальных машинах с операционными системами Windows требуется установить пакет VMware Tools версии 11.0.1. При установке пакета VMware Tools нужно установить компонент

NSX File Introspection Driver, который входит в состав пакета, по умолчанию компонент NSX File Introspection Driver не устанавливается.

Для установки компонента NSX File Introspection Driver на виртуальных машинах с операционными системами Linux предусмотрены специальные пакеты. См. подробнее в документации к продуктам VMware https://docs.vmware.com.

Развертывание службы Guest Introspection

Для функционирования Kaspersky Security требуется развернуть службу Guest Introspection на каждом кластере VMware, на котором будут развернуты SVM с компонентом Защита от файловых угроз.

В результате развертывания службы Guest Introspection на кластере VMware служебные виртуальные машины Guest Introspection разворачиваются на каждом гипервизоре, входящем в состав кластера.

Развертывание службы Guest Introspection выполняется в консоли VMware vSphere Web Client.

► *Чтобы развернуть службу Guest Introspection, выполните следующие действия:*

1. В консоли VMware vSphere Web Client запустите мастер развертывания сетевых служб и служб обеспечения защиты виртуальных машин (раздел **Networking & Security** → **Installation and Upgrade** закладка **Service Deployments**).
2. С помощью мастера укажите следующие параметры развертывания службы Guest Introspection:
   a. Выберите в таблице службу Guest Introspection.
   b. Выберите один или несколько кластеров VMware, на которых вы хотите установить компонент Защита от файловых угроз.
   c. Если требуется, измените заданные по умолчанию параметры для всех служебных виртуальных машин Guest Introspection, которые будут развернуты на гипервизорах в составе выбранного кластера VMware:
      - Сеть, которую будут использовать служебные виртуальные машины.
      - Хранилище для развертывания служебных виртуальных машин.
      - Способ назначения IP-адресов. По умолчанию служебные виртуальные машины получают сетевые параметры по протоколу DHCP. Вы можете настроить статический пул IP-адресов, из которого будут назначаться IP-адреса служебных виртуальных машин.
3. Завершите работу мастера и дождитесь завершения развертывания службы Guest Introspection.

   Служебная виртуальная машина Guest Introspection будет развернута на каждом гипервизоре в составе кластера VMware, который вы выбрали.

Подробнее о процедуре развертывания службы Guest Introspection см. в Базе знаний http://support.kaspersky.ru/15288.

Учетные записи для установки и работы программы

Учетная запись для установки плагина управления Kaspersky Security и Сервера интеграции

Для установки плагина управления Kaspersky Security и Сервера интеграции (см. раздел "Установка основного плагина управления Kaspersky Security и Сервера интеграции" на стр. 40) требуется учетная

запись, которая обладает правами на установку программного обеспечения (например, учетная запись из группы локальных администраторов).

Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен Active Directory®, для подключения к Серверу интеграции требуется доменная учетная запись, которая входит в группу KLAdmins, или учетная запись, которая входит в группу локальных администраторов.

Для предотвращения несанкционированного доступа рекомендуется обеспечить безопасность учетной записи, которая используется для подключения к Серверу интеграции.

Учетные записи для развертывания, удаления SVM и работы программы

Для развертывания и удаления SVM с компонентами программы Kaspersky Security требуются следующие учетные записи:

- Учетная запись VMware vCenter Server, которой назначена предустановленная системная роль ReadOnly. Для обеспечения возможности проверки выключенных виртуальных машин нужно назначить этой учетной записи следующие права:
  - Virtual machine → Change Configuration → Add existing disk
  - Virtual machine → Change Configuration → Add or remove device
  - Virtual machine → Change Configuration → Remove disk
  - ESX Agent Manager → Modify
- Учетная запись VMware NSX Manager, которой назначена роль Enterprise Administrator.
- Если вы хотите использовать программу Kaspersky Security для защиты виртуальной инфраструктуры под управлением VMware vCloud Director, также требуется учетная запись VMware vCloud Director, которая обладает следующими правами:
  - General → Perform administrator queries
  - Organization → View Organizations

Роли должны быть назначены учетным записям на верхнем уровне иерархии объектов виртуальной инфраструктуры VMware.

О создании учетных записей в инфраструктуре VMware см. в документации VMware.

Учетная запись для подключения Сервера интеграции к Kaspersky Security Center

Эта учетная запись используется, если программа работает в режиме multitenancy.

Сервер интеграции подключается к Kaspersky Security Center, чтобы получить информацию о виртуальных Серверах администрирования, созданных в Kaspersky Security Center, и установить соответствие между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования. Для подключения Сервера интеграции к Kaspersky Security Center требуется учетная запись, которая должна обладать правами на чтение в функциональной области **Базовая функциональность** → **Виртуальные Серверы администрирования**.

Вы можете создать и настроить учетную запись для подключения Сервера интеграции к Kaspersky Security Center в окне свойств Сервера администрирования Kaspersky Security Center в разделе **Безопасность**.

По умолчанию раздел **Безопасность** не отображается в окне свойств Сервера администрирования. Чтобы включить отображение раздела **Безопасность**, требуется установить флажок **Отображать разделы с параметрами безопасности** в окне **Настройка интерфейса** (меню **Вид** → **Настройка интерфейса**) и перезапустить Консоль администрирования Kaspersky Security Center.

Подробнее о правах учетных записей в Kaspersky Security Center см. в документации Kaspersky Security Center.

Используемые порты

Для установки и работы компонентов программы в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика между виртуальными машинами, требуется открыть порты, описанные в таблице ниже.

Таблица 1. Порты, используемые программой

Порт и протокол	Направление	Назначение и описание
13000, 14000 TCP	От SVM к Серверу администрирования Kaspersky Security Center.	Для управления программой через Kaspersky Security Center.
15000 UDP	От Сервера администрирования Kaspersky Security Center к SVM.	Для управления программой через Kaspersky Security Center.
13291 TCP	От Консоли администрирования Kaspersky Security Center к Серверу администрирования Kaspersky Security Center.	Для подключения Консоли администрирования к Серверу администрирования Kaspersky Security Center.
22 TCP	От Сервера интеграции к SVM.	Для взаимодействия SVM и Сервера интеграции.
7271 TCP	От SVM к Серверу интеграции.	Для взаимодействия SVM и Сервера интеграции.
7271 TCP	От VMware NSX Manager к Серверу интеграции.	Для взаимодействия VMware NSX Manager и Сервера интеграции.
443 TCP	От Сервера интеграции к VMware NSX Manager.	Для взаимодействия Сервера интеграции с виртуальной инфраструктурой.
443 TCP	От Сервера интеграции к серверам управления виртуальной инфраструктурой (VMware vCenter Server и VMware vCloud Director).	Для взаимодействия Сервера интеграции с виртуальной инфраструктурой.

kaspersky

Подготовка образа SVM

Программа Kaspersky Security поставляется в виде бинарных компонентов. Перед началом установки программы необходимо создать образ SVM с установленным компонентом Защита от файловых угроз, используя поставляемый вспомогательный диск с необходимыми пакетами.

Аппаратные и программные требования для создания образа:

- Гипервизор VMware ESXi 6.7.0, 14320388.
- Минимум 4 ГБ оперативной памяти под виртуальную машину.
- Минимум 40 Гб дискового пространства на виртуальной машине.

► *Чтобы создать образ SVM с установленным компонентом Защита от файловых угроз, выполните следующие действия:*

1. Создайте виртуальную машину с установленной операционной системой CentOS 7.0.
2. Войдите в систему на созданной виртуальной машине под учетной записью root.
3. Установите из CentOS-репозитория утилиты:

   ```
   yum install -y sudo kpartx qemu-img wget unzip parted e2fsprogs psmisc net-tools python-lxml ftp createrepo perl perl-XML-LibXML
   ```

4. Скопируйте в папку /tmp/ все файлы из списка 1 (см. ниже).
5. Установите VMware OvfTool с помощью команды:

   ```
   cd /tmp/
   sh VMware-ovftool-4.3.0-7948156-lin.x86_64.bundle --console --required --eulas-agreed
   ```

6. Распакуйте скрипты для изготовления образа виртуальной машины защиты при помощи команды:

   ```
   cd /tmp/
   tar xzf build-ova6-cert.tgz -C /root/
   ```

7. Скопируйте в папку /root/build-ova6-cert/input все файлы из списка 2 (см. ниже).
8. Скопируйте в папку /root/build-ova6-cert/input все файлы из списка 3 (см. ниже).
9. Запустите скрипт подготовки сборочной директории:

   ```
   cd /root/build-ova6-cert
   ./unpack.sh
   ```

10. Запустите скрипт сборки образа виртуальной машины:

    ```
    cd /root/build-ova6-cert
    ./run.sh
    ```

11. Дождитесь успешного завершения команды.

Результатом сборки являются следующие файлы:

- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_2gb.mf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_2gb.ovf

- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_4gb.mf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_4gb.ovf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_8gb.mf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.2cpu_8gb.ovf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.4cpu_4gb.mf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.4cpu_4gb.ovf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.4cpu_8gb.mf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.4cpu_8gb.ovf
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7.appinfo.xml
- /root/build-ova6-cert/output/iso/ksv-6.0.0-1629.x86_64.el7-disk1.vmdk

Список 1

1. VMware-ovftool-4.3.0-7948156-lin.x86_64.bundle
2. build-ova6-cert.tgz

Список 2

1. centos_repo.tar.gz
2. centos-release-7-7.1908.0.el7.centos.x86_64.rpm
3. ntfs-3g-2017.3.23-1.el7.x86_64.rpm
4. vmware-studio-vami-tools_2.5.0.0-387333_x86_64.rpm

Список 3

1. ksv_all.esm
2. klnagent64-11.0.0-37.x86_64.rpm
3. ksv-6.0.0-1491.x86_64.rpm
4. ksv_epsec-6.0.0-1491.x86_64.rpm
5. ksv_ksn-6.0.0-1491.x86_64.rpm
6. ksv-tools-6.0.0-1491.x86_64.rpm
7. ksv-6.0-xml.tgz
8. integrity_check.xml

kaspersky

Установка программы

Установка программы Kaspersky Security состоит из следующих этапов:

1. Установка плагина (или плагинов) управления Kaspersky Security и Сервера интеграции.

   Независимо от выбранного варианта использования программы (в режиме multitenancy или для защиты виртуальной инфраструктуры под управлением одного или нескольких автономных серверов VMware vCenter Server) вам нужно установить основной плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции (см. раздел "Установка основного плагина управления Kaspersky Security и Сервера интеграции" на стр. 40).

   Если вы хотите использовать программу в режиме multitenancy, вам нужно также установить плагин управления Kaspersky Security для клиентов (см. раздел "Установка плагина управления Kaspersky Security для клиентов" на стр. 42).

   При первом запуске Консоли администрирования Kaspersky Security Center после установки плагинов управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. Мастер позволяет создать политики по умолчанию и задачи (см. раздел "Политики и задачи по умолчанию" на стр. 45).

   > Если мастер первоначальной настройки управляемой программы не запустился автоматически, рекомендуется запустить его вручную (см. раздел "Запуск мастера первоначальной настройки управляемой программы" на стр. 44). Политики по умолчанию позволяют сразу после установки программы обеспечить регистрацию событий и отображение защищаемых виртуальных машин в Консоли администрирования Kaspersky Security Center.

2. Настройка параметров подключения Сервера интеграции к одному или нескольким серверам управления виртуальной инфраструктурой (см. раздел "Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой" на стр. 49).

3. Регистрация в VMware NSX Manager службы Kaspersky File Antimalware Protection (см. раздел "Регистрация службы Kaspersky File Antimalware Protection" на стр. 51).

   Чтобы установить компонент Защита от файловых угроз, вам нужно зарегистрировать службу защиты файловой системы (Kaspersky File Antimalware Protection).

   Ввод параметров, необходимых для регистрации и развертывания службы Kaspersky File Antimalware Protection, выполняется в мастере, который запускается из Консоли Сервера интеграции. По окончании ввода параметров Сервер интеграции выполняет регистрацию службы в VMware NSX Manager.

   В консоли VMware vSphere Web Client вы можете убедиться в том, что регистрация службы Kaspersky File Antimalware Protection завершилась успешно (см. раздел "Просмотр зарегистрированных служб в консоли VMware vSphere Web Client" на стр. 55).

4. Развертывание SVM с компонентом Защита от файловых угроз на гипервизорах VMware ESXi (см. раздел "Развертывание SVM с компонентом Защита от файловых угроз" на стр. 56). Развертывание SVM выполняется в консоли VMware vSphere Web Client.

   После развертывания SVM Сервер интеграции передает на каждую новую SVM параметры конфигурации, которые вы указали при регистрации службы Kaspersky File Antimalware Protection.

   Kaspersky Security Center помещает развернутые SVM в кластеры KSC (см. раздел "Концепция управления программой через Kaspersky Security Center" на стр. 17).

5. Настройка групп безопасности NSX (NSX Security Group) и политик безопасности NSX (NSX Security Policy).

Чтобы защищать виртуальные машины, вам нужно выполнить следующие действия в консоли VMware vSphere Web Client:

a. Включить виртуальные машины в одну или несколько групп безопасности NSX (NSX Security Group) (см. раздел "Настройка групп безопасности NSX (NSX Security Group)" на стр. 57).

b. Настроить одну или несколько политик безопасности NSX (NSX Security Policy) и применить политики безопасности на группы безопасности NSX (см. раздел "Настройка и применение политик безопасности NSX (NSX Security Policy)" на стр. 57).

6. Подготовка программы к работе (см. раздел "Подготовка программы к работе. Включение защиты виртуальных машин" на стр. 65):

   После установки программы требуется активировать программу, обновить базы программы на всех новых SVM и настроить параметры работы программы с помощью политики.

Если вы хотите использовать программу в режиме multitenancy, после установки программы вам нужно настроить защиту организаций-клиентов (см. раздел "Настройка защиты организаций-клиентов" на стр. 58).

В этом разделе

Установка основного плагина управления Kaspersky Security и Сервера интеграции

Установку плагина управления Kaspersky Security и компонентов Сервера интеграции следует выполнять под учетной записью, которая обладает правами на установку программного обеспечения (например, под учетной записью из группы локальных администраторов).

Для установки Сервера интеграции, Консоли Сервера интеграции и плагина управления Kaspersky Security требуется платформа Microsoft .NET Framework 4.6.1. Вы можете установить платформу Microsoft .NET Framework 4.6.1 предварительно или она будет установлена автоматически в ходе установки компонентов программы Kaspersky Security. В случае проблем с установкой Microsoft .NET Framework 4.6.1 убедитесь, что на компьютере установлены обновления Windows KB2919442 и KB2919355.

Перед началом установки основного плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции рекомендуется закрыть Консоль администрирования Kaspersky Security Center.

► *Чтобы установить основной плагин управления Kaspersky Security и компоненты Сервера интеграции с помощью мастера, выполните следующие действия:*

1. На компьютере, где установлены Консоль администрирования и Сервер администрирования Kaspersky Security Center, запустите файл ksv-components_6.0.0.369_mlg.exe. Этот файл входит в комплект поставки.

   Если на компьютере не установлен Сервер администрирования Kaspersky Security Center, на этом компьютере не будет установлен Сервер интеграции. Будет установлен только плагин управления Kaspersky Security и Консоль Сервера интеграции.

   Запустится мастер установки.

2. Выберите язык локализации мастера и компонентов Kaspersky Security и перейдите к следующему шагу мастера.

   По умолчанию в окне используется язык локализации операционной системы, установленной на компьютере, где запущен мастер.

3. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения установки требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в окне мастера.

   Перейдите к следующему шагу мастера.

4. Если на компьютере, на котором запущен мастер, установлен Сервер администрирования Kaspersky Security Center и этот компьютер не входит в домен Active Directory, вам требуется создать пароль учетной записи администратора Сервера интеграции. Для управления Сервером интеграции будет использоваться учетная запись администратора Сервера интеграции *admin*.

   Введите пароль в полях **Пароль** и **Подтверждение пароля**. Имя учетной записи недоступно для изменения.

   Пароль должен содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: ! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~. В целях безопасности рекомендуется задавать пароль длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

   Перейдите к следующему шагу мастера.

5. Если на компьютере, на котором запущен мастер, установлен Сервер администрирования Kaspersky Security Center и порт 7271, используемый по умолчанию для подключения к Серверу интеграции, занят, вам требуется указать номер порта для подключения к Серверу интеграции.

   В поле **Порт** укажите номер порта из диапазона 1025–65536 и перейдите к следующему шагу мастера.

6. Просмотрите информацию о действиях, которые выполнит мастер, и нажмите на кнопку **Далее**, чтобы начать выполнение перечисленных действий.

7. Дождитесь завершения работы мастера.

   Если в ходе работы мастера возникает ошибка, мастер выполняет откат внесенных изменений.

8. Нажмите на кнопку **Завершить**, чтобы закрыть окно мастера.

Если ранее в вашей виртуальной инфраструктуре был установлен Сервер интеграции и при его удалении вы сохранили данные, используемые в работе Сервера интеграции, эти данные используются автоматически при повторной установке Сервера интеграции.

После завершения установки плагина управления Kaspersky Security и Сервера интеграции в Консоли администрирования Kaspersky Security Center в блоке **Развертывание** отображается ссылка для запуска Консоли Сервера интеграции. Установленный плагин управления Kaspersky Security отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

Для взаимодействия Сервера интеграции с Консолью администрирования, с SVM, с сервером VMware vCenter Server и VMware NSX Manager используется защищенное SSL-соединение.

Для устранения известных уязвимостей операционной системы для протокола SSL при установке Сервера интеграции в реестр операционной системы вносятся изменения, описанные в базе технической поддержки Microsoft (см. раздел Ограничение использования криптографических алгоритмов и протоколов на странице http://support.microsoft.com/kb/245030). В результате этих изменений отключаются следующие криптографические шифры и протоколы:

- SSL 3.0;
- SSL 2.0;
- AES 128;
- RC2 40/56/128;
- RC4 40/56/64/128;
- 3DES 168.

В ходе установки Сервера интеграции в реестре операционной системы устанавливается самоподписанный SSL-сертификат Сервера интеграции, который используется для установки защищенного соединения с Сервером интеграции. Если вы хотите использовать более надежный сертификат, вы можете заменить SSL-сертификат Сервера интеграции (процедура замены сертификата описана в Базе знаний http://support.kaspersky.ru/15283).

Установка плагина управления Kaspersky Security для клиентов

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

Установку плагина управления Kaspersky Security для клиентов следует выполнять под учетной записью, которая обладает правами на установку программного обеспечения (например, под учетной записью из группы локальных администраторов).

Перед началом установки плагина управления Kaspersky Security для клиентов рекомендуется закрыть Консоль администрирования Kaspersky Security Center.

► *Чтобы установить плагин управления Kaspersky Security для клиентов, выполните следующие действия:*

1. На компьютере, где установлена Консоль администрирования Kaspersky Security Center, запустите файл ksv-t-components_6.0.0.277_mlg.exe. Этот файл входит в комплект поставки.

   Запустится мастер установки плагина управления Kaspersky Security для клиентов.

2. Выберите язык локализации мастера и плагина управления Kaspersky Security для клиентов и перейдите к следующему шагу мастера.

   По умолчанию в окне используется язык локализации операционной системы, установленной на компьютере, где запущен мастер.

3. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения установки требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в окне мастера.

   Перейдите к следующему шагу мастера.

4. Просмотрите информацию о действиях, которые выполнит мастер, и нажмите на кнопку **Далее**, чтобы начать выполнение перечисленных действий.

5. Дождитесь завершения работы мастера.

   Если в ходе работы мастера возникает ошибка, мастер выполняет откат внесенных изменений.

6. Нажмите на кнопку **Завершить**, чтобы закрыть окно мастера.

Результат установки плагинов управления и Сервера интеграции

В результате установки основного плагина управления Kaspersky Security и компонентов Сервера интеграции выполняются следующие действия:

1. В Консоли администрирования Kaspersky Security Center создается ссылка для запуска Консоли Сервера интеграции: **Управление Kaspersky Security для виртуальных сред 6.0 Защита без агента**. Ссылка отображается в рабочей области узла **Сервер администрирования** на закладке **Мониторинг** в блоке **Развертывание**.

2. При первом запуске Консоли администрирования Kaspersky Security Center после установки плагина управления запускается мастер первоначальной настройки управляемой программы, который создает в папке **Управляемые устройства** главного Сервера администрирования основную политику и задачи по умолчанию (см. раздел "Политики и задачи по умолчанию" на стр. 45). Мастер также может быть запущен вручную (см. раздел "Запуск мастера первоначальной настройки управляемой программы" на стр. 44).

3. Основной плагин управления Kaspersky Security отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

В результате установки плагина управления Kaspersky Security для клиентов выполняются следующие действия:

1. При первом запуске Консоли администрирования Kaspersky Security Center после установки плагина управления запускается мастер первоначальной настройки управляемой программы, который создает в папке **Управляемые устройства** главного Сервера администрирования политику для клиентов по умолчанию (см. раздел "Политики и задачи по умолчанию" на стр. 45). Мастер также может быть запущен вручную (см. раздел "Запуск мастера первоначальной настройки управляемой программы" на стр. 44).
2. Плагин управления Kaspersky Security для клиентов отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

► *Чтобы посмотреть список установленных плагинов управления, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования**.
2. Откройте окно свойств Сервера администрирования одним из следующих способов:
   - в контекстном меню узла выберите пункт **Свойства**;
   - в рабочей области в блоке **Сервер администрирования** перейдите по ссылке **Свойства Сервера администрирования**.

   Откроется окно **Свойства: Сервер администрирования**.
3. В окне свойств Сервера администрирования в разделе **Дополнительно** выберите подраздел **Информация об установленных плагинах управления программами**.

   В правой части окна в списке установленных плагинов управления отображается основной плагин управления Kaspersky Security: **Kaspersky Security для виртуальных сред 6.0 Защита без агента**.

   Если вы установили плагин управления Kaspersky Security для клиентов, также отображается **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)**.

Запуск мастера первоначальной настройки управляемой программы

При первом запуске Консоли администрирования Kaspersky Security Center после установки основного плагина управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. В результате работы мастера в папке **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center автоматически создаются основная политика по умолчанию, задача обновления баз программы и задача полной проверки для виртуальных машин, которые не входят в организации vCloud Director (см. раздел "Политики и задачи по умолчанию" на стр. 45).

Если вы также установили плагин управления Kaspersky Security для клиентов, мастер первоначальной настройки управляемой программы запускается повторно и автоматически создает в папке **Управляемые устройства** главного Сервера администрирования политику для клиентов по умолчанию (см. раздел "Политики и задачи по умолчанию" на стр. 45).

Политика для клиентов по умолчанию не создается автоматически на виртуальном Сервере администрирования Kaspersky Security Center.

Если мастер первоначальной настройки управляемой программы не запустился автоматически, рекомендуется запустить его вручную. Политики по умолчанию позволяют сразу после установки программы обеспечить регистрацию событий и отображение защищаемых виртуальных машин в Консоли администрирования Kaspersky Security Center.

► *Чтобы запустить вручную мастер первоначальной настройки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования**.
2. В контекстном меню узла выберите пункт **Все задачи → Мастер первоначальной настройки управляемой программы**.
3. Нажмите на кнопку **Далее** в окне приветствия.
4. На следующем шаге выберите управляемую программу: **Kaspersky Security для виртуальных сред 6.0 Защита без агента** и нажмите на кнопку **Далее**.
5. Дождитесь окончания работы и закройте окно мастера.
6. Если вы используете программу в режиме multitenancy, выполните повторно шаги 1–3, на следующем шаге выберите управляемую программу: **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** и нажмите на кнопку **Далее**.
7. Дождитесь окончания работы и закройте окно мастера.

Политики и задачи по умолчанию

В результате работы мастера первоначальной настройки управляемой программы в папке **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center создаются следующие политики и задачи.

Основная политика по умолчанию

Политика отображается в рабочей области папки **Управляемые устройства** главного Сервера администрирования на закладке **Политики** и имеет название **Политика по умолчанию KSV Agentless 6.0**.

Параметры политики по умолчанию принимают следующие значения:

- Защита от файловых угроз выключена (объектам защищаемой инфраструктуры не назначен профиль защиты).
- SNMP-мониторинг состояния SVM выключен.
- Использование резервного хранилища включено. Срок хранения резервных копий файлов составляет 30 дней.
- Использование Kaspersky Security Network выключено.

Если вы хотите использовать основную политику по умолчанию для защиты виртуальных машин, вам нужно включить антивирусную защиту в этой политике.

Все параметры основной политики по умолчанию разрешено переопределять в политиках вложенного уровня иерархии (все "замки" открыты).

Наличие основной политики по умолчанию позволяет сразу после развертывания SVM и до того, как вы создадите политику вручную, использовать следующие возможности Kaspersky Security Center:

- отображение списка защищаемых виртуальных машин в свойствах кластера KSC;
- регистрация событий, происходящих во время проверки и защиты виртуальных машин, которые не входят в состав организаций vCloud Director;
- отображение в отчете о ключах сведений о виртуальных машинах, для защиты которых используются лицензионные ключи;
- отображение в отчете о состоянии защиты информации о защищаемых виртуальных машинах.

Если вы хотите удалить основную политику по умолчанию, убедитесь, что на всех SVM применяется одна из созданных вами основных политик. Если на SVM не применяется основная политика, в Kaspersky Security Center не регистрируются события от этой SVM, происходящие во время проверки и защиты виртуальных машин, которые не входят в состав организаций vCloud Director, а также эти виртуальные машины не отображаются в отчетах.

Политика для клиентов по умолчанию

Эта политика создается, только на главном Сервере администрирования Kaspersky Security Center, если вы установили плагин управления Kaspersky Security для клиентов.

Политика отображается в рабочей области папки **Управляемые устройства** главного Сервера администрирования на закладке **Политики** и имеет название **Политика по умолчанию KSV Agentless 6.0 (для клиентов)**.

Параметры этой политики не используются непосредственно для защиты виртуальных машин. Но параметры основного профиля защиты и параметры использования KSN, настроенные в этой политике, могут наследоваться в политиках для клиентов, расположенных во вложенных группах администрирования, например, в папке **Управляемые устройства** виртуального Сервера администрирования.

Все параметры политики для клиентов по умолчанию разрешено переопределять в политиках вложенного уровня иерархии (все "замки" открыты).

Наличие политики для клиентов в папке **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center является необходимым условием для регистрации событий, происходящих во время проверки и защиты виртуальных машин клиентов, а также отображения виртуальных машин клиентов в составе защищаемой инфраструктуры кластера KSC и в списке виртуальных машин, находящихся под защитой SVM.

В политике для клиентов по умолчанию вы можете настраивать параметры уведомлений о событиях, происходящих во время проверки и защиты виртуальных машин клиентов (см. раздел "Настройка параметров уведомлений о событиях" на стр. 134).

Задача обновления баз по умолчанию

Задача отображается в рабочей области папки **Управляемые устройства** главного Сервера администрирования на закладке **Задачи** и имеет название **Обновление баз программы**.

Задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center и позволяет обновлять базы на всех SVM. (см. раздел "Обновление баз программы" на стр. 125)

Задача полной проверки по умолчанию

Задача отображается в рабочей области папки **Управляемые устройства** главного Сервера администрирования на закладке **Задачи** и имеет название **Задача полной проверки по умолчанию**.

Задача позволяет проверять все виртуальные машины, которые находятся в составе всей защищаемой инфраструктуры и не входят в организации vCloud Director.

Параметры задачи полной проверки принимают следующие значения:

- Уровень безопасности – **Рекомендуемый**:
  - Проверка архивов выключена.
  - Проверка самораспаковывающихся архивов и вложенных OLE-объектов включена.
  - Kaspersky Security не проверяет составные файлы, размер которых превышает значение 8 МБ.
  - Время проверки файла не ограничено.
  - Kaspersky Security проверяет файлы виртуальных машин на наличие вирусов, червей, троянских программ, вредоносных утилит, программ автодозвона, рекламных программ и многократно упакованных файлов.
- Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.
- Kaspersky Security не проверяет выключенные виртуальные машины, шаблоны виртуальных машин и файлы на оптических дисках.
- Выполнение задачи проверки прекращается по истечении 120 минут с момента запуска задачи.
- Исключения из области проверки не заданы.

Вы можете запускать эту задачу вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

Настройка Сервера интеграции

После установки Сервера интеграции необходимо настроить параметры подключения Сервера интеграции к виртуальной инфраструктуре.

Настройка параметров Сервера интеграции выполняется в Консоли Сервера интеграции.

kaspersky

В этом разделе

Запуск Консоли Сервера интеграции

Если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен Active Directory, убедитесь в том, что ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции.

► *Чтобы запустить Консоль Сервера интеграции, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования**.
2. Запустите Консоль Сервера интеграции по ссылке **Управление Kaspersky Security для виртуальных сред 6.0 Защита без агента** на закладке **Мониторинг** в блоке **Развертывание**.
3. Если выполняется одно из следующих условий, откроется окно для ввода параметров подключения к Серверу интеграции:
   - если компьютер, на котором установлена Консоль Сервера интеграции, не входит в домен Active Directory;
   - если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен, но не удалось подключиться к Серверу интеграции, используя адрес и порт подключения, заданные в параметрах Консоли Сервера интеграции.

   Укажите следующие параметры подключения:
   - Адрес и порт Сервера интеграции, к которому выполняется подключение.
   - Учетную запись для подключения к Серверу интеграции:
     - Если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, вы можете использовать доменную учетную запись. Для этого установите флажок **Использовать доменную учетную запись**.

       Если вы хотите использовать учетную запись администратора Сервера интеграции (admin), введите пароль администратора в поле **Пароль**.
     - Если компьютер, на котором установлена Консоль Сервера интеграции, не входит в домен или компьютер входит в домен, но ваша доменная учетная запись не входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, вы можете использовать только учетную запись администратора Сервера интеграции (admin). Введите пароль администратора Сервера интеграции в поле **Пароль**.

   Нажмите на кнопку **Подключить**.

4. Консоль проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат не является доверенным или не соответствует ранее установленному сертификату, откроется окно **Проверка сертификата** с сообщением об этом. По ссылке в окне вы можете посмотреть информацию о полученном сертификате. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

   Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Считать сертификат доверенным** в окне **Проверка сертификата**. Полученный сертификат будет установлен в качестве доверенного. Сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль Сервера интеграции.

Откроется Консоль Сервера интеграции.

Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой

В зависимости от виртуальной инфраструктуры, которую вы хотите защищать с помощью программы Kaspersky Security, вам нужно настроить подключение к следующим серверам управления виртуальной инфраструктурой:

- для защиты виртуальной инфраструктуры под управлением одного или нескольких серверов VMware vCenter Server вам нужно настроить подключение Сервера интеграции к каждому из этих серверов VMware vCenter Server;
- для защиты виртуальной инфраструктуры под управлением серверов VMware vCenter Server, подключенных к серверу VMware vCloud Director, вам нужно настроить подключение Сервера интеграции к каждому из этих серверов VMware vCenter Server, а также к серверу VMware vCloud Director.

Подключение к каждому серверу управления виртуальной инфраструктурой выполняется отдельно.

В инфраструктуре под управлением VMware vCloud Director вы можете подключать Сервер интеграции к серверам VMware vCenter Server и VMware vCloud Director в произвольном порядке. Сервер интеграции автоматически определяет, является ли каждый добавленный сервер VMware vCenter Server автономным или он подключен к серверу VMware vCloud Director.

► *Чтобы настроить параметры подключения Сервера интеграции к серверу управления виртуальной инфраструктурой, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).
2. В разделе **Защита виртуальной инфраструктуры** нажмите на кнопку **Добавить**.
3. В открывшемся окне **Подключение к виртуальной инфраструктуре** выберите тип сервера управления виртуальной инфраструктурой, к которому требуется настроить подключение, и нажмите на кнопку **Далее**.
4. Укажите следующие параметры:
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера управления виртуальной инфраструктурой, к которому подключается Сервер интеграции;
   - имя и пароль учетной записи, под которой Сервер интеграции подключается к серверу управления виртуальной инфраструктурой.

Введенные параметры подключения (кроме пароля) сохраняются в реестре операционной системы в защищенном виде.

5. Нажмите на кнопку **Проверить**. Сервер интеграции проверяет указанные параметры подключения и SSL-сертификат, полученный от сервера управления виртуальной инфраструктурой. Если подключиться не удалось или во время подключения обнаружены ошибки сертификата, в окне отображается сообщение об ошибке.

   Если ошибка подключения происходит потому, что сертификат, полученный от сервера управления виртуальной инфраструктурой, не является доверенным для Сервера интеграции, откроется окно **Подтверждение сертификата**. Если полученный сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и установить подключение. Для этого в открывшемся окне нажмите на кнопку **Установить сертификат**. Полученный сертификат сохраняется в качестве доверенного для Сервера интеграции.

   Доверенными для Сервера интеграции считаются также сертификаты, которые являются доверенными в операционной системе, в которой установлен Сервер интеграции.

   При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

6. После установки соединения с сервером управления виртуальной инфраструктурой нажмите на кнопку **ОК** в окне **Подключение к виртуальной инфраструктуре**, чтобы закрыть окно.

   Введенный адрес или имя сервера управления виртуальной инфраструктурой отображается в таблице в разделе **Защита виртуальной инфраструктуры**.

   Если вы настроили подключение к серверу VMware vCloud Director и подключенным к нему серверам VMware vCenter Server, строки с информацией об этих серверах VMware vCenter Server автоматически группируются в список, расположенный под строкой этого VMware vCloud Director.

Для каждого сервера управления виртуальной инфраструктурой в таблице отображается список действий, которые вы можете выполнить при настройке подключения к этому серверу и для дальнейшего развертывания защиты виртуальной инфраструктуры. Вы можете развернуть или свернуть список возможных действий щелчком левой клавиши мыши по адресу или имени сервера управления виртуальной инфраструктурой в графе **Адрес**.

Если требуется, вы можете изменить или удалить ранее введенные параметры подключения Сервера интеграции к серверу управления виртуальной инфраструктурой.

► *Чтобы изменить параметры подключения Сервера интеграции к серверу управления виртуальной инфраструктурой, выполните следующие действия:*

1. Разверните список возможных действий для выбранного сервера управления виртуальной инфраструктурой щелчком левой клавиши мыши по адресу или имени сервера управления виртуальной инфраструктурой в графе **Адрес**.
2. В зависимости от типа сервера управления виртуальной инфраструктурой выберите действие **Изменить параметры подключения к VMware vCenter Server** или **Изменить параметры подключения к VMware vCloud Director**. Откроется окно **Подключение к виртуальной инфраструктуре**.

3. Введите новые параметры подключения и выполните проверку возможности подключения, как описано в процедуре настройки параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой (см. пункты 4–6 предыдущей инструкции).

► *Чтобы удалить параметры подключения Сервера интеграции к серверу управления виртуальной инфраструктурой, выполните следующие действия:*

1. Разверните список возможных действий для выбранного сервера управления виртуальной инфраструктурой щелчком левой клавиши мыши по адресу или имени сервера управления виртуальной инфраструктурой в графе **Адрес**.
2. В зависимости от типа сервера управления виртуальной инфраструктурой выберите действие **Удалить VMware vCenter Server из списка** или **Удалить VMware vCloud Director из списка**.
3. Подтвердите удаление в открывшемся окне.

   В инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager удаление сервера VMware vCenter Server из списка возможно, только если службы Kaspersky Security не зарегистрированы в VMware NSX Manager.

После настройки подключения Сервера интеграции к одному или нескольким серверам VMware vCenter Server вы можете перейти к развертыванию защиты в виртуальной инфраструктуре VMware.

Регистрация службы Kaspersky File Antimalware Protection

После настройки подключения Сервера интеграции к серверу VMware vCenter Server вам требуется запустить процедуру регистрации служб Kaspersky Security и ввести параметры, необходимые для выполнения следующих этапов установки программы:

- регистрации в VMware NSX Manager службы защиты файловой системы (Kaspersky File Antimalware Protection);
- развертывания службы Kaspersky File Antimalware Protection;
- первоначальной настройки конфигурации новых SVM после развертывания службы Kaspersky File Antimalware Protection.

Регистрацию службы Kaspersky File Antimalware Protection в VMware NSX Manager и настройку конфигурации новых SVM выполняет Сервер интеграции.

► *Чтобы ввести параметры, необходимые для регистрации и развертывания службы Kaspersky File Antimalware Protection, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).

   Откроется раздел **Защита виртуальной инфраструктуры**.
2. В списке выберите сервер VMware vCenter Server и разверните список доступных действий щелчком левой клавиши мыши по адресу или имени VMware vCenter Server в графе **Адрес**.
3. В блоке **Управление защитой** выберите действие **Зарегистрировать службы Kaspersky Security**.

Запустится мастер ввода параметров, необходимых для регистрации и развертывания службы Kaspersky File Antimalware Protection. Следуйте указаниям мастера.

В этом разделе

Подключение к VMware NSX Manager

На этом шаге укажите параметры подключения Сервера интеграции к VMware NSX Manager:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) VMware NSX Manager;
- имя и пароль учетной записи, под которой производится подключение к VMware NSX Manager. Этой учетной записи должна быть назначена роль Enterprise Administrator.

Также на этом шаге вы можете настроить параметры, которые использует VMware NSX Manager для передачи информации на Сервер интеграции. По умолчанию установлены параметры, которые Консоль Сервера интеграции использовала при подключении к Серверу интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48). В поле **Адрес** указано полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции (если компьютер находится в домене), имя компьютера в рабочей группе Windows (если компьютер не входит в домен) или IP-адрес компьютера.

Убедитесь, что VMware NSX Manager сможет подключиться к Серверу интеграции, используя параметры, установленные по умолчанию, или измените эти параметры. Чтобы изменить параметры, установите флажок **Указать параметры подключения VMware NSX Manager к Серверу интеграции** и укажите IP-адрес или полное доменное имя компьютера, на котором установлен Сервер интеграции, и порт для подключения.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к VMware NSX Manager и к Серверу интеграции с указанными параметрами.

Во время подключения к VMware NSX Manager мастер проверяет SSL-сертификат, полученный от VMware NSX Manager. Если полученный сертификат содержит ошибку, в окне мастера отображается сообщение об ошибке. Вы можете посмотреть информацию о полученном сертификате по ссылке **Посмотреть сертификат**.

Если ошибка подключения происходит потому, что сертификат, полученный от VMware NSX Manager, не является доверенным для Сервера интеграции, но полученный сертификат соответствует политике безопасности вашей организации, вы можете подтвердить подлинность сертификата и установить подключение. Для этого нажмите на кнопку **Установить сертификат**. Полученный сертификат сохраняется в качестве доверенного для Сервера интеграции.

Доверенными для Сервера интеграции считаются также сертификаты, которые являются доверенными в операционной системе, в которой установлен Сервер интеграции.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Если проверка параметров подключения к Серверу интеграции завершилась с ошибкой, в окне мастера отображается сообщение об ошибке, переход к следующему шагу мастера невозможен. Если вы хотите исправить введенные параметры, нажмите на кнопку **Отмена**. Если параметры введены правильно, вы можете игнорировать сообщение об ошибке. В этом случае нажмите на кнопку **Продолжить**, чтобы перейти к следующему шагу мастера.

Выбор образа SVM с компонентом Защита от файловых угроз

На этом шаге укажите образ SVM с установленным компонентом Защита от файловых угроз. Сервер интеграции зарегистрирует службу защиты файловой системы (Kaspersky File Antimalware Protection) в VMware NSX Manager. После завершения регистрации вы можете выполнить развертывание службы защиты файловой системы на кластерах VMware. В результате на гипервизорах будут развернуты SVM с компонентом Защита от файловых угроз.

В комплект поставки программы входит несколько образов SVM с установленным компонентом Защита от файловых угроз, с помощью которых вы можете развернуть SVM нужной конфигурации (по количеству выделенных для SVM процессоров и оперативной памяти).

Все файлы образа SVM с установленным компонентом Защита от файловых угроз должны быть расположены в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS.

► *Чтобы указать образ SVM, выполните следующие действия:*

1. Укажите в поле адрес файла описания образов SVM (файла в формате XML) или адрес OVF-файла образа SVM, соответствующего нужной конфигурации SVM.
2. Нажмите на кнопку **Проверить**.

   Мастер проверит образ SVM. Если образ поврежден или версия образа не поддерживается, мастер отобразит сообщение об ошибке.

   Если проверка образа SVM завершилась успешно, в нижней части окна отображается следующая информация о выбранном образе SVM:

   - **Конфигурация SVM** – количество выделенных для SVM процессоров и оперативной памяти.

     Если вы указали адрес файла описания образов SVM (файла в формате XML), вы можете выбрать нужную конфигурацию SVM в раскрывающемся списке в поле **Конфигурация SVM**.
   - **Название программы** – название программы, которая установлена на SVM.
   - **Версия SVM** – номер версии SVM.
   - **Производитель** – производитель программы, которая установлена на SVM.

- **Описание** – краткое описание программы.
- **Необходимое место на диске** – объем дискового пространства, которое требуется для развертывания SVM в хранилище данных.

Если вы не хотите устанавливать компонент Защита от файловых угроз, снимите флажок **Зарегистрировать службу защиты файловой системы**.

Перейдите к следующему шагу мастера.

Настройка параметров подключений для SVM

На этом шаге укажите IP-адрес Сервера администрирования Kaspersky Security Center и SSL-порт, которые SVM будет использовать для подключения к Kaspersky Security Center.

Также на этом шаге вы можете настроить параметры для подключения SVM к Серверу интеграции. По умолчанию установлены параметры, которые Консоль Сервера интеграции использовала при подключении к Серверу интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48). В поле **Адрес** указано полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции (если компьютер находится в домене), имя компьютера в рабочей группе Windows (если компьютер не входит в домен) или IP-адрес компьютера.

Убедитесь, что SVM сможет подключиться к Серверу интеграции, используя параметры, установленные по умолчанию, или измените эти параметры. Чтобы изменить параметры, установите флажок **Указать параметры подключения SVM к Серверу интеграции** и укажите IP-адрес или полное доменное имя компьютера, на котором установлен Сервер интеграции, и порт для подключения.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к Kaspersky Security Center и к Серверу интеграции с указанными параметрами.

Если проверка параметров подключения завершилась с ошибкой, в окне мастера отображается сообщение об ошибке, переход к следующему шагу мастера невозможен. Если вы хотите исправить введенные параметры, нажмите на кнопку **Отмена**. Если параметры введены правильно, вы можете игнорировать сообщение об ошибке. В этом случае нажмите на кнопку **Продолжить**, чтобы перейти к следующему шагу мастера.

Создание паролей учетных записей на SVM

На этом шаге создайте пароль учетной записи klconfig (пароль конфигурирования) и пароль учетной записи root на SVM. Пароль конфигурирования требуется для изменения конфигурации SVM. Учетная запись root используется для доступа к операционной системе на SVM и к файлам трассировки SVM.

Введите пароль для каждой учетной записи в полях **Пароль** и **Подтверждение пароля**.

Пароли должны содержать не более 60 символов. Вы можете использовать только символы латинского алфавита (прописные и строчные буквы), цифры, а также следующие специальные символы: `! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~`. В целях безопасности рекомендуется задавать пароли длиной не менее 8 символов и использовать хотя бы три из четырех категорий символов: строчные буквы, прописные буквы, цифры и специальные символы.

Перейдите к следующему шагу мастера.

Выбор часового пояса для SVM

На этом шаге вы можете выбрать часовой пояс, который будет использоваться на всех SVM. По умолчанию часовой пояс для SVM соответствует часовому поясу, заданному на компьютере, на котором установлена Консоль Сервера интеграции.

Если требуется изменить часовой пояс для SVM, выберите значение в раскрывающемся списке.

Перейдите к следующему шагу мастера.

Подтверждение параметров

На этом шаге проверьте введенные параметры службы Kaspersky File Antimalware Protection.

Перейдите к следующему шагу мастера, чтобы запустить регистрацию службы Kaspersky File Antimalware Protection.

Процесс регистрации службы Kaspersky File Antimalware Protection

На этом шаге отображается информация о действиях, которые выполняет Сервер интеграции, чтобы зарегистрировать службу Kaspersky File Antimalware Protection и подготовить параметры конфигурации, которые будут переданы на новые SVM после их развертывания.

Если в ходе выполнения действия произошла ошибка, информация об этом отображается в окне мастера. Мастер выполняет откат внесенных изменений.

После выполнения всех действий перейдите к следующему шагу мастера.

Завершение работы мастера

На этом шаге отображается информация о результате регистрации службы Kaspersky File Antimalware Protection.

Если регистрация службы завершилась успешно, завершите работу мастера.

Если регистрация службы завершилась с ошибкой, мастер отображает информацию об ошибке. В этом случае завершите работу мастера, устраните причину ошибки и начните процедуру заново.

Просмотр зарегистрированных служб в консоли VMware vSphere Web Client

Регистрацию службы Kaspersky File Antimalware Protection в VMware NSX Manager выполняет Сервер интеграции.

Вы можете посмотреть список зарегистрированных служб в консоли VMware vSphere Web Client в разделе **Networking & Security** → **Service Definitions** на закладке **Services**.

Сервер интеграции регистрируется в VMware NSX Manager как Kaspersky Service Manager.

Вы можете посмотреть список зарегистрированных Service Manager в консоли VMware vSphere Web Client в разделе **Networking & Security** → **Service Definitions** на закладке **Service Managers**.

Подробнее о просмотре зарегистрированных служб и Service Manager см. в Базе знаний http://support.kaspersky.ru/15288.

Развертывание SVM с компонентом Защита от файловых угроз

SVM с компонентом Защита от файловых угроз разворачиваются на гипервизорах VMware ESXi в результате развертывания службы защиты файловой системы(Kaspersky File Antimalware Protection) на кластерах VMware. Развертывание службы выполняется в консоли VMware vSphere Web Client.

► *Чтобы развернуть SVM с компонентом Защита от файловых угроз, выполните следующие действия:*

1. В консоли VMware vSphere Web Client запустите мастер развертывания сетевых служб и служб обеспечения защиты виртуальных машин (раздел **Networking & Security** → **Installation**, закладка **Service Deployments**).
2. С помощью мастера укажите следующие параметры:
   a. Выберите в таблице службу Kaspersky File Antimalware Protection.
   b. Выберите один или несколько кластеров VMware, на которых вы хотите развернуть SVM.
   c. Если требуется, измените заданные по умолчанию параметры для всех SVM, которые будут развернуты на гипервизорах в составе выбранного кластера VMware:
      - Сеть, которую будут использовать SVM.
      - Хранилище для развертывания SVM.
      - Способ назначения IP-адресов. По умолчанию SVM получают сетевые параметры по протоколу DHCP. Вы можете настроить статический пул IP-адресов, из которого будут назначаться IP-адреса SVM.
3. Завершите работу мастера и дождитесь завершения развертывания службы Kaspersky File Antimalware Protection.

   SVM с компонентом Защита от файловых угроз будет развернута на каждом гипервизоре в составе кластера VMware, который вы выбрали.

Подробнее о процедуре развертывания SVM с компонентом Защита от файловых угроз см. в Базе знаний http://support.kaspersky.ru/15288.

kaspersky

Настройка групп безопасности NSX (NSX Security Group)

Настройка групп безопасности NSX (NSX Security Group) выполняется в консоли VMware vSphere Web Client. Вам требуется включить в одну или несколько групп безопасности NSX все виртуальные машины, которые вы хотите защищать с помощью программы Kaspersky Security.

► *Чтобы настроить группу безопасности NSX, выполните следующие действия:*

1. В консоли VMware vSphere Web Client запустите мастер создания группы безопасности NSX в разделе **Networking & Security** → **Service Composer** на закладке **Security Groups**.
2. С помощью мастера введите название новой группы безопасности NSX (например, "Kaspersky Security Group" или "Protected by Kaspersky") и настройте правила включения виртуальных машин в группу.

   Предусмотрены следующие способы включения виртуальных машин в группу безопасности NSX:

   - Динамическое включение виртуальных машин в группу безопасности NSX. В группу входят все виртуальные машины, которые удовлетворяют указанным критериям.
   - Включение в группу безопасности NSX указанных объектов виртуальной инфраструктуры VMware. Вы можете выбрать объекты, которые должны входить в состав группы, например: объект Datacenter, кластер VMware, ресурсный пул, отдельные виртуальные машины. По умолчанию в группу включаются все дочерние объекты указанного объекта. При этом вы можете указать отдельные объекты виртуальной инфраструктуры, которые должны быть исключены из группы безопасности NSX.

   Вы можете сочетать эти способы при настройке правил включения виртуальных машин в группу безопасности NSX. Например, настроить динамическое включение виртуальных машин в группу по определенному критерию и указать объекты управления VMware, которые должны быть исключены из группы.

Подробнее о настройке групп безопасности NSX см. в Базе знаний http://support.kaspersky.ru/15288.

Настройка и применение политик безопасности NSX (NSX Security Policy)

Настройка политик безопасности NSX (NSX Security Policy) выполняется в консоли VMware vSphere Web Client. Настроенные политики безопасности NSX требуется назначить для ранее созданных групп безопасности NSX (NSX Security Group).

В каждой политике безопасности NSX вам требуется настроить использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

► *Чтобы настроить и применить политику безопасности NSX, выполните следующие действия:*

1. В консоли VMware vSphere Web Client запустите мастер создания политики безопасности NSX в разделе **Networking & Security** → **Service Composer** на закладке **Security Policies**.
2. На шаге мастера **Guest Introspection Services** добавьте службу Kaspersky File Antimalware Protection с произвольным именем и действием по умолчанию (*Apply*).
3. Завершите работу мастера создания политики безопасности NSX.

4. В списке политик безопасности NSX на закладке **Security Policies** примените политику (**Apply**) на группу безопасности NSX, в которую включены защищаемые виртуальные машины.

Подробнее о настройке политик безопасности NSX см. в Базе знаний http://support.kaspersky.ru/15288.

Настройка защиты организаций-клиентов

Действия, описанные в этом разделе, необходимо выполнять, только если вы хотите использовать программу в режиме multitenancy.

Чтобы настроить защиту организаций-клиентов, после установки программы вам нужно выполнить следующие действия:

1. В Консоли администрирования Kaspersky Security Center для каждого клиента, виртуальные машины которого требуется защищать, создать виртуальный Сервер администрирования и учетную запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования (см. раздел "Создание виртуального Сервера администрирования для клиента" на стр. 59).
2. В Консоли администрирования Kaspersky Security Center создать учетную запись, под которой Сервер интеграции будет подключаться к Серверу администрирования Kaspersky Security Center (см. раздел "Учетные записи для установки и работы программы" на стр. 34). Подключение требуется для получения информации о виртуальных Серверах администрирования, созданных в Kaspersky Security Center, и для настройки соответствий между виртуальными Серверами администрирования и организациями vCloud Director, которые содержат виртуальные машины клиентов.
3. В Консоли Сервера интеграции выполнить подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center (см. раздел "Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 60) и настроить список соответствий между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).

   Если для организации vCloud Director не установлено соответствие с виртуальным Сервером администрирования, программа Kaspersky Security не защищает виртуальные машины, которые входят в эту организацию vCloud Director.
4. Передать администратору клиента следующую информацию:
   - адрес Сервера интеграции;
   - адрес виртуального Сервера администрирования, настроенного для этого клиента;
   - имя и пароль учетной записи для подключения к виртуальному Серверу администрирования.
5. Убедиться в том, что программа подготовлена к работе и настроены политики для защиты виртуальной инфраструктуры каждого клиента (см. раздел "Подготовка программы к работе. Включение защиты виртуальных машин" на стр. 65): для защиты от файловых угроз на каждом виртуальном Сервере администрирования Kaspersky Security Center, соответствующем организации-клиенту, должна быть настроена политика для клиентов.

kaspersky

В этом разделе

Создание виртуального Сервера администрирования для клиента

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

Виртуальный Сервер администрирования требуется для управления защитой виртуальных машин, входящих в состав организации vCloud Director.

Виртуальный Сервер администрирования нужно создавать во вложенной папке **Серверы администрирования** в группе администрирования, которая содержит кластер "VMware vCloud Director Agentless". Кластер должен соответствовать серверу VMware vCloud Director, под управлением которого находится организация vCloud Director, содержащая виртуальные машины клиента.

► *Чтобы создать виртуальный Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, которая содержит кластер "VMware vCloud Director Agentless", затем выберите вложенную папку **Серверы администрирования**.
2. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

   Запустится мастер добавления виртуального Сервера администрирования.
3. На первом шаге мастера укажите имя создаваемого виртуального Сервера администрирования.

   Имя виртуального Сервера администрирования не может содержать более 255 символов и специальные символы: `" * < > ? \ : |`.

   Перейдите к следующему шагу мастера.
4. Укажите адрес Сервера администрирования Kaspersky Security Center, на котором создается виртуальный Сервер администрирования, и перейдите к следующему шагу мастера.
5. Укажите учетную запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования. Вы можете указать ранее созданную учетную запись внутреннего пользователя Kaspersky Security Center или создать учетную запись с помощью кнопки **Создать**.

   Перейдите к следующему шагу мастера.
6. Запустите создание виртуального Сервера администрирования с помощью кнопки **Далее**.

7. На следующем шаге снимите флажок **Все пакеты** (для работы программы не требуются инсталляционные пакеты), перейдите к следующему шагу и завершите работу мастера.

В дереве консоли будет создан узел с именем **Сервер администрирования – <имя виртуального Сервера>**.

Подробнее о работе с виртуальными Серверами администрирования см. в документации Kaspersky Security Center.

Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center требуется для получения информации о виртуальных Серверах администрирования, созданных в Kaspersky Security Center.

► *Чтобы подключить Сервер интеграции к Серверу администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).
2. В списке слева выберите раздел **Управление защитой организаций-клиентов**.
3. В блоке **Параметры подключения к Kaspersky Security Center** укажите параметры подключения:
   - IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера администрирования Kaspersky Security Center.
   - Имя и пароль учетной записи, под которой Сервер интеграции должен подключаться к Серверу администрирования Kaspersky Security Center (см. раздел "Учетные записи для установки и работы программы" на стр. 34).
4. Нажмите на кнопку **Подключить**. Статус подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center отображается в блоке **Статус подключения к Kaspersky Security Center** в верхней части окна.

После подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center вы можете устанавливать соответствия между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования.

Если подключение было установлено ранее и вы хотите изменить параметры подключения, вы можете прервать текущее подключение с помощью кнопки **Отключить**, расположенную в блоке **Статус подключения к Kaspersky Security Center**, и затем подключиться с новыми параметрами.

Если в состав Сервера администрирования Kaspersky Security Center входит один или несколько виртуальных Серверов администрирования, для которых установлено соответствие с организациями vCloud Director, при попытке отменить подключение отображается предупреждение. Если подключение отсутствует, невозможно установить новые соответствия между виртуальными Серверами администрирования и организациями vCloud Director. Ранее установленные соответствия сохраняются.

kaspersky

Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования выполняется в Консоли Сервера интеграции. В списке соответствий вы можете выполнять следующие действия:

- устанавливать соответствия между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center (см. раздел "Установка соответствия между организацией vCloud Director и виртуальным Сервером администрирования" на стр. 62);
- просматривать список установленных соответствий;
- отменять установленные соответствия (см. раздел "Отмена соответствия между организацией vCloud Director и виртуальным Сервером администрирования" на стр. 63).

► *Чтобы открыть список соответствий между организациями vCloud Director и виртуальными Серверами администрирования, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).
2. В списке слева выберите раздел **Управление защитой организаций-клиентов** и убедитесь, что Сервер интеграции подключен к Серверу администрирования Kaspersky Security Center. Выполните подключение, если подключение не установлено (см. раздел "Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 60).

   Если Сервер интеграции не подключен к Серверу администрирования Kaspersky Security Center, вы не можете устанавливать новые соответствия между виртуальными Серверами администрирования и организациями vCloud Director. Ранее установленные соответствия сохраняются, вы можете их отменять.

3. Откройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования одним из следующих способов:

   - В разделе **Защита виртуальной инфраструктуры** разверните список доступных действий для сервера VMware vCloud Director, под управлением которого находится организация vCloud Director, и перейдите по ссылке **Установить соответствия для организаций vCloud Director**. Откроется список соответствий для организаций vCloud Director, которые находятся под управлением одного сервера VMware vCloud Director.
   - В разделе **Управление защитой организаций-клиентов** нажмите на кнопку **Открыть список**, расположенную в блоке **Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования**. Откроется список соответствий для организаций vCloud Director, которые находятся под управлением всех серверов VMware vCloud Director.

   Откроется окно **Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования**.

Список соответствий отображается в виде таблицы. В каждой строке таблицы содержатся следующие данные:

- **Виртуальный Сервер** – имя виртуального Сервера администрирования, которому соответствует организация из графы **Организация vCloud Director**. Если соответствие с организацией vCloud Director для этого виртуального Сервера администрирования не установлено, в графе отображается значение *нет*.
- **Организация vCloud Director** – имя организации vCloud Director, которой соответствует виртуальный Сервер администрирования из графы **Виртуальный Сервер**. Если соответствие с виртуальным Сервером администрирования для этой организации vCloud Director не установлено, в графе отображается значение *нет*.
- **VMware vCloud Director** – IP-адрес или имя сервера VMware vCloud Director, под управлением которого находится организация из графы **Организация vCloud Director**. Если организация vCloud Director в этой строке таблицы не указана, в графе отображается значение *нет*.

При просмотре списка соответствий вы можете использовать следующие возможности:

- Фильтр. Чтобы применить фильтр, вы можете использовать следующие ссылки, расположенные над таблицей:
  - **Все** – показывать в таблице все строки. Это значение выбрано по умолчанию.
  - **Соответствие установлено** – показывать только строки, в которых отображается имя организации vCloud Director и имя виртуального Сервера администрирования, между которыми установлено соответствие.
  - **Соответствие не установлено** – показывать только строки, в которых отображается имя организации vCloud Director или имя виртуального Сервера администрирования, для которых соответствия не установлены.
- Поиск по любой графе таблицы. Вы можете ввести условие поиска в поисковой строке, расположенной над таблицей, чтобы найти организацию vCloud Director, виртуальный Сервер администрирования или сервер VMware vCloud Director. Поиск инициируется во время ввода символов. В таблице отображаются все строки, в которых присутствует значение, удовлетворяющее условиям поиска. Чтобы сбросить результаты поиска, нужно удалить содержимое строки поиска.

В этом разделе

Установка соответствия между организацией vCloud Director и виртуальным Сервером администрирования

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

► *Чтобы установить соответствие между организацией vCloud Director и виртуальным Сервером администрирования, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).
2. Выберите раздел **Управление защитой организаций-клиентов** и убедитесь, что Сервер интеграции подключен к Серверу администрирования Kaspersky Security Center. Выполните подключение, если подключение не установлено (см. раздел "Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center" на стр. 60).
3. Откройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).
4. Выполните одно из следующих действий:
   - Если вы хотите установить соответствие для организации vCloud Director, найдите в таблице строку, которая содержит имя организации vCloud Director, и перейдите по ссылке, расположенной в графе **Виртуальный Сервер**.

     Откроется окно **Выбор виртуального Сервера администрирования**. В окне отображается список всех виртуальных Серверов администрирования, для которых еще не установлено соответствие с организацией vCloud Director.
   - Если вы хотите установить соответствие для виртуального Сервера администрирования, найдите в таблице строку, которая содержит имя виртуального Сервера администрирования, и перейдите по ссылке, расположенной в графе **Организация vCloud Director**. Откроется окно **Выбор организации vCloud Director**. В окне отображается список всех организаций vCloud Director, для которых еще не установлено соответствие с виртуальным Сервером администрирования. Список организаций vCloud Director сгруппирован по серверам VMware vCloud Director.

   Для поиска нужной строки в таблице вы можете использовать фильтр или поисковую строку (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).
5. В открывшемся окне выберите виртуальный Сервер администрирования или организацию vCloud Director и нажмите на кнопку **ОК**.

   Окно выбора закроется, новое соответствие отобразится в окне **Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования**.

Отмена соответствия между организацией vCloud Director и виртуальным Сервером администрирования

Действия, описанные в этом разделе, необходимо выполнять, только если вы используете программу в режиме multitenancy.

Если организация vCloud Director удалена из VMware vCloud Director или виртуальные машины, которые входят в организацию vCloud Director, больше не требуется защищать, вы можете отменить ранее установленное соответствие между организацией vCloud Director и виртуальным Сервером администрирования.

► *Чтобы отменить соответствие между организацией vCloud Director и виртуальным Сервером администрирования, выполните следующие действия:*

1. Запустите Консоль Сервера интеграции (см. раздел "Запуск Консоли Сервера интеграции" на стр. 48).
2. Откройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования (см. раздел "Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования" на стр. 61).
3. Найдите в таблице строку, которая содержит организацию vCloud Director и виртуальный Сервер администрирования, соответствие между которыми вы хотите отменить.

   Для поиска нужной строки в таблице вы можете использовать фильтр или поисковую строку.
4. Нажмите на значок  , расположенный в строке, и подтвердите отмену соответствия в открывшемся окне.
5. Закройте окно **Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования**.

Если для организации vCloud Director не установлено соответствие с виртуальным Сервером администрирования, программа Kaspersky Security не защищает виртуальные машины, которые входят в эту организацию vCloud Director.

kaspersky

Подготовка программы к работе. Включение защиты виртуальных машин

После установки программы требуется выполнить следующие действия:

- Активировать программу на всех новых SVM (см. раздел "Процедура активации программы" на стр. 68).
- Обновить базы программы на всех новых SVM (см. раздел "Процедура обновления баз программы" на стр. 69).
- Включить защиту виртуальных машин от файловых угроз с помощью политики. По умолчанию Kaspersky Security не защищает виртуальные машины.

Для защиты от файловых угроз виртуальных машин, которые не входят в состав организаций vCloud Director, вы можете использовать основную политику по умолчанию (см. раздел "Политики и задачи по умолчанию" на стр. 45) или создать основную политику (см. раздел "Создание основной политики" на стр. 70).

Если программа работает в режиме multitenancy, для защиты виртуальной инфраструктуры клиентов от файловых угроз требуется создать политику для клиентов на каждом виртуальном Сервере администрирования Kaspersky Security Center, соответствующем организации-клиенту (см. раздел "Создание политики для клиентов" на стр. 73). Создать политику для клиентов может администратор провайдера или администратор клиента (см. раздел "Инструкция по работе с программой для администратора организации-клиента" на стр. 136).

Чтобы защищать виртуальную машину от файловых угроз, нужно назначить виртуальной машине профиль защиты (см. раздел "О профилях защиты Kaspersky Security" на стр. 20). Виртуальная машина, которой не назначен профиль защиты, исключается из защиты.

Профиль защиты может назначаться непосредственно объектам виртуальной инфраструктуры (включая виртуальные машины) (см. раздел "Назначение профилей защиты объектам виртуальной инфраструктуры" на стр. 96) или путем установки соответствия между профилем защиты и конфигурацией профиля NSX (NSX Profile Configuration), действие которой распространяется на виртуальные машины (см. раздел "Назначение профилей защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)" на стр. 97).

Вы можете назначать основной профиль защиты, который формируется автоматически при создании политики, или создавать и назначать дополнительные профили защиты, если вы хотите использовать разные параметры защиты для разных объектов виртуальной инфраструктуры. Назначение профилей выполняется в свойствах политики.

Kaspersky Security защищает только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин от файловых угроз (см. раздел "Защита виртуальных машин от файловых угроз" на стр. 83).

Если на SVM программа не активирована или отсутствуют базы программы, Kaspersky Security не защищает виртуальные машины.

kaspersky

В этом разделе

Об активации программы

Активация программы – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Чтобы активировать программу, требуется добавить лицензионный ключ на все SVM. Для добавления ключа на SVM используется *задача активации программы*.

При создании задачи активации программы используется ключ из хранилища ключей Kaspersky Security Center.

Рекомендуется добавлять ключ в хранилище ключей Kaspersky Security Center с помощью файла ключа. *Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского".

Ключ также может быть добавлен с помощью кода активации. *Код активации* – это уникальная последовательность из двадцати латинских букв и цифр.

Использование кода активации для добавления ключа в хранилище ключей Kaspersky Security Center может привести к выходу программы из сертифицированного состояния.

Информацию о ключах, добавленных на SVM, вы можете посмотреть в Консоли администрирования Kaspersky Security Center:

- в папке **Лицензии Лаборатории Касперского** дерева консоли;
- в свойствах программы, установленной на SVM;
- в свойствах задачи активации программы;
- в отчете об использовании ключей.

Особенности добавления ключей разных типов

Для Kaspersky Security предусмотрены следующие *схемы лицензирования:*

- Лицензирование по количеству виртуальных машин, защищаемых с помощью программы. Для этой схемы лицензирования используются ключи для серверов и ключи для рабочих станций (в зависимости

от типа операционной системы защищаемых виртуальных машин). В соответствии с лицензионным ограничением программа используется для защиты определенного количества виртуальных машин.

- Лицензирование по количеству ядер, используемых в физических процессорах на всех гипервизорах, на которых установлены SVM. Для этой схемы лицензирования используются ключи с ограничением по ядрам. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, развернутых на гипервизорах, в которых используется определенное количество ядер физических процессоров.
- Лицензирование по количеству процессоров, используемых на гипервизорах, на которых работают защищенные виртуальные машины. Для этой схемы лицензирования используются ключи с ограничением по процессорам. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, развернутых на гипервизорах, в которых используется определенное количество процессоров.

Для защиты виртуальных машин с гостевыми операционными системами Linux вы можете использовать только ключи для серверов или ключи с ограничением по ядрам или процессорам.

При добавлении ключей следует учитывать следующие особенности:

- Если вы используете схему лицензирования по количеству защищаемых виртуальных машин, тип ключа, с помощью которого вы активируете программу, должен соответствовать типу гостевой операционной системы виртуальных машин:
  - для защиты виртуальных машин с операционными системами для серверов нужно добавить на SVM ключ для серверов;
  - для защиты виртуальных машин с операционными системами для рабочих станций нужно добавить на SVM ключ для рабочих станций;
  - для защиты виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций нужно добавить на SVM два ключа: ключ для серверов и ключ для рабочих станций.

  Если вы используете схему лицензирования по количеству ядер процессоров или по количеству процессоров, вам требуется один ключ (с ограничением по ядрам или с ограничением по процессорам) независимо от типа операционной системы, установленной на виртуальных машинах.

  Для защиты виртуальных машин с гостевыми операционными системами Linux вы можете использовать только ключи для серверов, ключи с ограничением по ядрам и ключи с ограничением по процессорам.

- Не поддерживается одновременное использование на SVM ключей, которые соответствуют разным схемам лицензирования. Если после активации программы вы добавляете ключ, который соответствует другой схеме лицензирования, то ранее добавленный ключ с SVM удаляется. Например, если вы добавляете ключ с ограничением по ядрам, а ранее на SVM был добавлен ключ для рабочих станций и / или ключ для серверов, то в результате выполнения задачи активный и (при наличии) дополнительный ключ для рабочих станций и / или ключ для серверов удаляются. Вместо них добавляется в качестве активного ключ с ограничением по ядрам.

  Вы можете одновременно использовать на SVM только ключи, соответствующие одной схеме лицензирования, например ключ для рабочих станций и ключ для серверов (схема лицензирования по количеству защищаемых виртуальных машин).

Ключ, удаленный с SVM, вы можете добавить на другую SVM, если не истек срок действия лицензии, связанной с ключом.

Процедура активации программы

После установки программы рекомендуется настроить задачу активации, которая будет автоматически запускаться на всех новых SVM сразу после их развертывания.

Если вы используете схему лицензирования по количеству защищаемых виртуальных машин, для защиты виртуальных машин и с серверной, и с настольной операционной системой вам нужно создать две задачи активации: для добавления серверного ключа на SVM и для добавления настольного ключа на SVM.

► *Чтобы настроить задачу активации, выполните следующие действия:*

1. Добавьте лицензионный ключ в хранилище ключей Kaspersky Security Center:
   a. Откройте Консоль администрирования Kaspersky Security Center и выберите в дереве консоли папку **Лицензии Лаборатории Касперского**.
   b. Нажмите на кнопку **Добавить код активации или ключ** в рабочей области. Запустится мастер добавления ключа в хранилище.
   c. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.
   d. Укажите путь к файлу ключа. Для этого нажмите на кнопку **Обзор** и в открывшемся окне выберите файл с расширением key.
   e. Снимите флажок **Автоматически распространять ключ на управляемые устройства** (возможность автоматического распространения ключей не поддерживается для программы Kaspersky Security). Перейдите к следующему шагу мастера.
   f. Завершите работу мастера добавления ключа в хранилище.
   g. Добавленный ключ отобразится в списке ключей в папке **Лицензии Лаборатории Касперского**.
2. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center.

   Вы можете создать задачу активации для SVM определенного кластера KSC. Для этого в папке **Управляемые устройства** выберите группу администрирования, содержащую этот кластер KSC.

   В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**. Запустится мастер создания задачи.
3. Укажите программу, для которой создается задача, и тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 6.0 Защита без агента** выберите **Активация программы**.

   Перейдите к следующему шагу мастера создания задачи.
4. Выберите ключ из хранилища ключей Kaspersky Security Center. Для этого нажмите на кнопку **Выбрать**. Откроется окно **Выбор лицензионного ключа**. Выберите ключ и нажмите на кнопку **ОК**.

   Перейдите к следующему шагу мастера создания задачи.

5. Настройте параметры расписания запуска задачи. Для задачи активации, которая будет автоматически запускаться на всех новых SVM сразу после их развертывания, рекомендуется настроить следующие параметры:

   - В раскрывающемся списке **Запуск по расписанию** выберите режим **Один раз**. В полях **Дата запуска** и **Время запуска** оставьте значения, установленные по умолчанию.
   - Установите флажок **Запускать пропущенные задачи**.

   Перейдите к следующему шагу мастера создания задачи.

6. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера создания задачи.
7. Завершите работу мастера.

Созданная задача активации программы отобразится в списке задач и будет запускаться в соответствии с настроенным расписанием. Если вы настроили расписание по рекомендации, задача будет запускаться на всех новых SVM сразу после их развертывания.

Вы можете просматривать информацию о результатах выполнения задачи в Консоли администрирования Kaspersky Security Center (см. раздел "О задачах Kaspersky Security" на стр. 24).

Процедура обновления баз программы

После установки плагина управления Kaspersky Security автоматически создается задача обновления баз программы. Эта задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center и позволяет обновлять базы программы на всех SVM. Вы можете использовать автоматически созданную задачу обновления баз программы. При необходимости вы можете изменить параметры этой задачи или удалить ее и настроить задачу обновления баз программы на SVM одного или нескольких кластеров KSC, входящих в одну группу администрирования.

► *Чтобы обновить базы программы, выполните следующие действия:*

1. Убедитесь в том, что в Kaspersky Security Center создана задача загрузки обновлений в хранилище (см. раздел "Обновление баз программы" на стр. 125). Если задача загрузки обновлений в хранилище отсутствует, создайте ее (см. в документации Kaspersky Security Center).
2. Дождитесь запуска по расписанию задачи загрузки обновлений в хранилище или запустите задачу вручную. Убедитесь в том, что задача загрузки обновлений в хранилище выполнена успешно (см. подробнее в документации Kaspersky Security Center).
3. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы.

   > Задача обновления баз программы, созданная автоматически после установки плагина управления Kaspersky Security, и находится на закладке **Задачи** в папке **Управляемые устройства**.

   Если задача обновления баз программы отсутствует, создайте ее (см. раздел "Настройка автоматического обновления баз программы" на стр. 125).
4. Дождитесь запуска по расписанию задачи обновления баз программы или запустите задачу вручную.
5. Убедитесь в том, что задача обновления баз программы выполнена успешно. Вы можете просматривать информацию о результатах выполнения задачи в Консоли администрирования Kaspersky Security Center.

После установки или обновления программы SVM передают в Kaspersky Security Center информацию о том, какие базы требуются для работы программы Kaspersky Security. Если на момент запуска задачи обновления баз программы Kaspersky Security Center еще не загрузил необходимые базы в хранилище, задача может завершиться с ошибкой. В этом случае вы можете вручную запустить задачу загрузки обновлений в хранилище, дождаться ее выполнения, а затем вручную запустить задачу обновления баз программы.

При обновлении баз программы Kaspersky Security проверяет их целостность. Если проверка закончилась неудачно, задача обновления баз программы завершается с ошибкой и Kaspersky Security продолжает использовать предыдущий набор баз программы. Если задача обновления баз программы завершается с ошибкой на новых SVM, рекомендуется обратиться в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 173). Если на SVM отсутствуют базы программы, Kaspersky Security не защищает виртуальные машины.

Создание основной политики

Основная политика определяет параметры защиты от файловых угроз для виртуальных машин, которые не входят в состав организаций vCloud Director.

► *Чтобы создать основную политику, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center запустите мастер создания политики:
   a. В дереве консоли выберите папку или группу администрирования, в которой вы хотите создать политику (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики** и нажмите на кнопку **Новая политика**.
2. На первом шаге мастера создания политики в списке выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента** и перейдите к следующему шагу мастера.
3. Введите название новой политики и перейдите к следующему шагу мастера.
4. Мастер выполняет подключение к Серверу интеграции для получения информации о виртуальной инфраструктуре VMware.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции по умолчанию используется ваша доменная учетная запись. Флажок **Использовать доменную учетную запись** установлен по умолчанию. Вы также можете использовать учетную запись администратора Сервера интеграции (admin). Для этого снимите флажок **Использовать доменную учетную запись** и введите пароль администратора в поле **Пароль**.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или компьютер входит в домен, но ваша доменная учетная запись не входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции вы можете использовать только учетную запись администратора Сервера интеграции (admin). Введите пароль администратора в поле **Пароль**.

Если для подключения к Серверу интеграции вы используете учетную запись администратора Сервера интеграции (admin), вы можете сохранить пароль администратора. Для этого установите флажок **Сохранить пароль**. При следующем подключении к этому Серверу интеграции используется сохраненный пароль администратора. Если вы снимаете флажок, установленный при предыдущем подключении к Серверу интеграции, Kaspersky Security удаляет ранее сохраненный пароль администратора Сервера интеграции.

Флажок **Сохранить пароль** может быть недоступен, если на компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, установлены обновления Windows KB 2992611 и / или KB 3000850. Чтобы восстановить возможность сохранения пароля администратора, вы можете удалить эти обновления Windows или внести изменения в реестр операционной системы, как описано в Базе знаний https://support.kaspersky.ru/15285.

Перейдите к следующему шагу мастера создания политики.

Мастер проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

После того, как подключение будет установлено, откроется окно **Выбор защищаемой инфраструктуры**. Выберите один из следующих вариантов:

- Если вы создаете политику в группе администрирования, которая содержит кластер "VMware vCenter Agentless", выберите вариант **Один сервер VMware vCenter Server**. Затем выберите в списке VMware vCenter Server, соответствующий этому кластеру KSC.

  Если выбранный VMware vCenter Server не соответствует группе администрирования в которой расположена политика, Kaspersky Security не защищает виртуальные машины.

- Если вы создаете политику в любой другой папке или группе администрирования, выберите вариант **Вся защищаемая инфраструктура**.

Нажмите на кнопку **ОК** в окне **Выбор защищаемой инфраструктуры**.

5. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты. Значения параметров основного профиля защиты, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского".

Если политика создается в группе, которая содержит кластер "VMware vCenter Agentless", основной профиль защиты назначается по умолчанию серверу VMware vCenter Server и наследуется всеми дочерними объектами виртуальной инфраструктуры.

Значения параметров, установленные по умолчанию, достаточны для первоначальной настройки программы. Во время работы с программой вы можете выполнить более тонкую настройку параметров основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 85).

Перейдите к следующему шагу мастера.

6. На этом шаге вы можете включить SNMP-мониторинг состояния SVM (см. раздел "SNMP-мониторинг состояния SVM" на стр. 131). По умолчанию SNMP-мониторинг выключен.

   Чтобы предотвратить несанкционированный доступ к службе SNMP, вы можете сформировать список IP-адресов, на которые агент SNMP должен передавать информацию о состоянии SVM.

   Перейдите к следующему шагу мастера.

7. Примите решение об участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 129).

   Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

   Если вы участвуете в Kaspersky Security Network, программа Kaspersky Security получает от служб KSN сведения о категории и репутации проверяемых файлов.

   В зависимости от расположения инфраструктуры KSN различают:

   - Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского".
   - Локальный KSN – инфраструктура расположена внутри корпоративной сети организации или на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера.

   Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

   Выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network**. Глобальный KSN не будет использоваться в работе программы.

   Если вы хотите использовать в работе программы Локальный KSN, установите флажок **Использовать Локальный KSN**.

   Если использование Локального KSN не настроено в Kaspersky Security Center, использовать Локальный KSN в работе программы невозможно. См. подробнее в документации Kaspersky Security Center.

   При необходимости позже вы сможете изменить параметры использования KSN в работе программы (см. раздел "Участие в Kaspersky Security Network" на стр. 129).

   Перейдите к следующему шагу мастера создания политики.

8. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик группы администрирования на закладке **Политики** и в папке **Политики** дерева консоли.

После создания политики вы можете назначить профили защиты виртуальным машинам, которые вы хотите защищать (см. раздел "Назначение профилей защиты объектам виртуальной инфраструктуры" на стр. 96).

В политике, расположенной в группе администрирования, которая содержит кластер "VMware vCenter Agentless", по умолчанию включена файловая защита (используется основной профиль защиты). В политиках, расположенных в папке **Управляемые устройства** или в группе администрирования, которая содержит кластер "VMware vCloud Director Agentless", файловая защита по умолчанию выключена.

Политика распространится на SVM после того, как Сервер администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security при следующем подключении SVM. Kaspersky Security начнет защищать виртуальные машины в соответствии с параметрами политики.

Если на SVM не добавлен лицензионный ключ или отсутствуют базы программы, SVM не защищает виртуальные машины.

Создание политики для клиентов

Политика для клиентов используется, только если программа работает в режиме multitenancy. Политика для клиентов позволяет настраивать параметры защиты от файловых угроз для виртуальных машин, которые входят в состав организаций vCloud Director.

► *Чтобы создать политику для клиентов, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center запустите мастер создания политики:
   a. В дереве консоли выберите папку или группу администрирования, в которой вы хотите создать политику (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики** и нажмите на кнопку **Новая политика**.
2. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** и перейдите к следующему шагу мастера.
3. Введите название новой политики и перейдите к следующему шагу мастера.
4. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера.

   Мастер выполняет подключение к Серверу интеграции для получения информации о виртуальной инфраструктуре VMware.

   Мастер проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата.

Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

5. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты. Значения параметров основного профиля защиты, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского".

   В политике, которая расположена в папке **Управляемые устройства** виртуального Сервера администрирования, основной профиль защиты назначается по умолчанию всем виртуальным машинам в составе защищаемой инфраструктуры клиента.

   Значения параметров, установленные по умолчанию, достаточны для первоначальной настройки программы. Во время работы с программой вы можете выполнить более тонкую настройку параметров основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 144).

   Перейдите к следующему шагу мастера.

6. Примите решение об участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 168). Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

   - Если вы хотите использовать KSN в работе программы и согласны со всеми пунктами Положения, выберите вариант **Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network**.
   - Если вы не хотите принимать участие в KSN, выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

   При необходимости позже вы сможете изменить свое решение (см. раздел "Участие в Kaspersky Security Network" на стр. 168).

   > Параметры использования KSN (тип и режим использования KSN) определяются основной политикой, в области действия которой находятся виртуальные машины клиента (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).

   Перейдите к следующему шагу мастера.

7. Завершите работу мастера создания политики.

Созданная политика для клиентов отобразится в списке политик группы администрирования на закладке **Политики** и в папке **Политики** дерева консоли.

В политике для клиентов, которая расположена в папке **Управляемые устройства** виртуального Сервера администрирования, по умолчанию включена файловая защита (используется основной профиль защиты). Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе

защищаемой инфраструктуры, вам нужно создать и назначить дополнительные профили защиты в свойствах политики (см. раздел "Назначение профиля защиты виртуальным машинам" на стр. 153).

В политике для клиентов, которая расположена в папке **Управляемые устройства** главного Сервера администрирования или в группе администрирования, которая содержит кластер "VMware vCloud Director Agentless", файловая защита по умолчанию выключена.

Политика распространится на SVM после того, как Сервер администрирования Kaspersky Security Center передаст информацию программе Kaspersky Security при следующем подключении SVM. Kaspersky Security начнет защищать виртуальные машины в соответствии с параметрами политики.

kaspersky

Процедура приемки

После установки программы перед ее вводом в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности и приведение конфигурации программы в соответствие с сертифицированной конфигурацией.

Установка программы завершилась успешно, если выполняются следующие условия:

1. На компьютере, где установлена Консоль администрирования Kaspersky Security Center, в списке установленных программ операционной системы отображается **Kaspersky Security для виртуальных сред 6.0 Защита без агента – компоненты управления**.
2. Если программа используется в режиме multitenancy:
   - на компьютере, где установлена Консоль администрирования Kaspersky Security Center, предназначенная для администратора провайдера антивирусной защиты, в списке установленных программ операционной системы отображается **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов) – плагин управления**;
   - на компьютере, где установлена Консоль администрирования Kaspersky Security Center, предназначенная для администратора клиента, в списке установленных программ операционной системы отображается **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов) – плагин управления**.
3. На компьютере, где установлен Сервер администрирования Kaspersky Security Center, в списке служб операционной системы присутствует служба **Сервер интеграции для Kaspersky Security для виртуальных сред** и эта служба запущена.
4. В Консоли администрирования Kaspersky Security Center в рабочей области узла **Сервер администрирования** на закладке **Мониторинг** в блоке **Развертывание** отображается ссылка для запуска Консоли Сервера интеграции. При переходе по ссылке запускается Консоль Сервера интеграции. После ввода параметров подключения происходит подключение к Серверу интеграции.
5. В Консоли администрирования Kaspersky Security Center в свойствах Сервера администрирования в списке установленных плагинов управления присутствует основной плагин управления Kaspersky Security (см. раздел "Установка основного плагина управления Kaspersky Security и Сервера интеграции" на стр. 40).
6. Если программа используется в режиме multitenancy:
   - в Консоли администрирования Kaspersky Security Center, предназначенной для администратора провайдера, в свойствах Сервера администрирования в списке установленных плагинов управления присутствует плагин управления Kaspersky Security для клиентов (см. раздел "Установка плагина управления Kaspersky Security для клиентов" на стр. 42).
   - в Консоли администрирования Kaspersky Security Center, предназначенной для администратора клиента, в свойствах Сервера администрирования в списке установленных плагинов управления присутствует плагин управления Kaspersky Security клиентов (см. раздел "Установка плагина Kaspersky Security для клиентов" на стр. 140).
7. В консоли VMware vSphere Web Client в разделе **Hosts and Clusters** отображается информация о том, что SVM успешно развернуты и находятся в состоянии **Powered On**.
8. В консоли VMware vSphere Web Client в разделе **Networking & Security** → **Installation and Upgrade** на закладке **Service Deployments** состояние (**Health status**) службы **Kaspersky File Antimalware Protection** отображается следующим образом: **Installation status** = **Succeeded**, **Service status** = **UP**.
9. В Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** дерева консоли присутствуют следующие группы администрирования:

- группа администрирования, название которой содержит IP-адрес или доменное имя сервера VMware vCenter Server – если SVM развернуты на гипервизорах VMware ESXi под управлением автономного сервера VMware vCenter Server;
- группа администрирования, название которой содержит IP-адрес или доменное имя сервера VMware vCloud Director – если SVM развернуты на гипервизорах VMware ESXi под управлением всех серверов VMware vCenter Server, подключенных к одному VMware vCloud Director.

10. Все развернутые SVM добавлены в эти группы администрирования: отображаются на закладке **Устройства** соответствующей группы администрирования и имеют статус **ОК** (зеленый).
11. Для каждой SVM в окне статистики отображается информация о лицензии и базах программы. Чтобы открыть окно статистики, выберите SVM на закладке **Устройства**, откройте окно свойств SVM, выберите раздел **Программы**, затем выберите в списке программу Kaspersky Security для виртуальных сред 6.0 Защита без агента и нажмите на кнопку **Статистика**.
12. В Консоли администрирования Kaspersky Security Center отображается информация о том, что задача активации и задача обновления баз программы завершены успешно на всех развернутых SVM. Список задач отображается на закладке **Задачи** в рабочей области папки **Управляемые устройства**. Вы можете посмотреть результаты выполнения задачи по ссылке **Посмотреть результаты**, расположенной справа от списка задач.
13. В Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** на закладке **Политики** присутствует основная политика в статусе **Активна**.
14. Если программа используется в режиме multitenancy, присутствуют следующие политики в статусе **Активна**:
    - политика для клиентов в папке **Управляемые устройства** в Консоли администрирования Kaspersky Security Center, предназначенной для администратора провайдера;
    - политика для клиентов в папке **Управляемые устройства** в Консоли администрирования Kaspersky Security Center, предназначенной для администратора клиента.

В этом разделе

Сертифицированное состояние программы

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

- Программа активирована на всех SVM (см. раздел "Процедура активации программы" на стр. 68).
- Базы программы обновлены на всех SVM (см. раздел "Процедура обновления баз программы" на стр. 69).
- Настроена основная политика, которая применяется на всех SVM (см. раздел "Создание основной политики" на стр. 70). Защита виртуальных машин включена в политике (см. раздел "Подготовка программы к работе. Включение защиты виртуальных машин" на стр. 65).
- Если программа используется в режиме multitenancy:
  - создана политика для клиентов по умолчанию на главном Сервере администрирования Kaspersky Security Center (см. раздел "Политики и задачи по умолчанию" на стр. 45);

  - настроена политика для клиентов на каждом виртуальном Сервере администрирования Kaspersky Security Center, соответствующем организации-клиенту (см. раздел "Создание политики" на стр. 141).
- Настроена задача полной проверки, созданная с помощью основного плагина управления в папке **Управляемые устройства** главного Сервера администрирования (см. раздел "Создание задачи полной проверки" на стр. 104).
- Если программа используется в режиме multitenancy: для каждого клиента настроена задача полной проверки, созданная с помощью плагина управления для клиентов в папке **Управляемые устройства** виртуального Сервера администрирования Kaspersky Security Center, соответствующего организации-клиенту (см. раздел "Создание задачи полной проверки" на стр. 156).
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Проверка работоспособности. Тестовый файл EICAR

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел "Процедура приемки" на стр. 76).
- Программа находится в сертифицированном состоянии (см. раздел "Сертифицированное состояние программы" на стр. 77).
- На виртуальной машине установлен Guest Introspection Thin Agent.
- Виртуальная машина включена в группу безопасности NSX (NSX Security Group), на эту группу безопасности применена политика безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

Проверка работоспособности функции защиты виртуальной машины

1. Выключите защиту виртуальной машины:
   a. Откройте свойства политики, в области действия которой находится виртуальная машина.
   b. Перейдите в подраздел **Защищаемая инфраструктура** и снимите флажок **Использовать защиту от файловых угроз**, расположенный в верхней части окна.

   > Эта операция требуется для успешного размещения на виртуальной машине тестового зараженного образца, иначе он будет мгновенно удален.

2. Разместите образец зараженного файла на виртуальной машине.

   В качестве тестового образца используется EICAR-файл, который можно получить на сайте http://www.eicar.org в разделе **Download**. Если вы скачали архив, его потребуется предварительно распаковать.

   Полученный файл поместите в новую папку на системном диске на виртуальной машине.
3. Очистите список событий на Сервере администрирования Kaspersky Security Center:
   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

b. В рабочей области перейдите на закладку **События**.

c. Выделите любое событие в списке, в контекстном меню выберите команду **Удалить все**.

> Эта операция требуется для обнуления данных в отчетах.

4. Включите защиту виртуальной машины:

   a. Откройте свойства политики, в области действия которой находится виртуальная машина.

   b. Перейдите в подраздел **Защищаемая инфраструктура** и установите флажок **Использовать защиту от файловых угроз**.

5. Проверьте доступ к зараженному файлу. Для этого попробуйте открыть подготовленный на виртуальной машине тестовый зараженный файл с помощью текстового редактора, например Блокнота.

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

6. Убедитесь, что зараженный файл был удален с виртуальной машины.

7. Проверьте наличие событий об обнаружении и удалении зараженного файла:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **События**.

   Ожидаемый результат: в списке присутствуют события об обнаружении зараженного файла и его успешном удалении.

8. Проверьте информацию в отчете об обнаруженных вирусах:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **Отчеты**.

   c. Выберите **Отчет об угрозах**. Сформированный отчет откроется в новом окне.

   d. Проверьте информацию в сводной и детальной таблицах отчета.

   Ожидаемый результат: в отчете зафиксирована корректная информация об обнаружении зараженного файла (время события, путь к файлу).

9. Проверьте информацию в отчете о зараженных устройствах:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **Отчеты**.

   c. Выберите **Отчет о наиболее заражаемых устройствах**. Сформированный отчет откроется в новом окне.

   d. Проверьте информацию в сводной и детальной таблицах отчета.

   Ожидаемый результат: в отчете зафиксирована корректная информация об обнаружении зараженного файла.

Проверка работоспособности функции проверки файлов виртуальной машины

1. Выключите защиту виртуальной машины:

a. Откройте свойства политики, в области действия которой находится виртуальная машина.

b. Перейдите в подраздел **Защищаемая инфраструктура** и снимите флажок **Использовать защиту от файловых угроз**, расположенный в верхней части окна.

> Эта операция требуется для успешного размещения на виртуальной машине тестового зараженного образца, иначе он будет мгновенно удален.

2. Разместите образец зараженного файла на виртуальной машине.

   В качестве тестового образца используется EICAR-файл, который можно получить на сайте http://www.eicar.org в разделе **Download**. Если вы скачали архив, его потребуется предварительно распаковать.

   Полученный файл поместите в новую папку на системном диске на виртуальной машине.

3. Очистите список событий на Сервере администрирования Kaspersky Security Center:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **События**.

   c. Выделите любое событие в списке, в контекстном меню выберите команду **Удалить все**.

> Эта операция требуется для обнуления данных в отчетах.

4. Откройте свойства ранее созданной задачи полной проверки и убедитесь, что в разделе **Параметры проверки** в блоке **Проверка включенных виртуальных машин** выбрано действие при обнаружении угрозы: **Лечить. Удалять, если лечение невозможно**.

5. Запустите задачу полной проверки. Для этого выберите задачу полной проверки в списке задач и в контекстном меню выберите команду **Запустить**.

   Ожидаемый результат: задача перешла в состояние **Выполняется**.

6. Дождитесь завершения задачи.

   Ожидаемый результат: задача завершилась успешно.

7. Убедитесь, что зараженный файл был удален с виртуальной машины.

8. Проверьте наличие событий об обнаружении и удалении зараженного файла:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **События**.

   Ожидаемый результат: в списке присутствуют события об обнаружении зараженного файла и его успешном удалении.

9. Проверьте информацию в отчете об обнаруженных вирусах:

   a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.

   b. В рабочей области перейдите на закладку **Отчеты**.

   c. Выберите **Отчет об угрозах**. Сформированный отчет откроется в новом окне.

   d. Проверьте информацию в сводной и детальной таблицах отчета.

Ожидаемый результат: в отчете зафиксирована корректная информация об обнаружении зараженного файла (время события, путь к файлу).

10. Проверьте информацию в отчете о зараженных устройствах:
    a. В Консоли администрирования Kaspersky Security Center выберите корневой узел **Сервер администрирования**.
    b. В рабочей области перейдите на закладку **Отчеты**.
    c. Выберите **Отчет о наиболее заражаемых устройствах**. Сформированный отчет откроется в новом окне.
    d. Проверьте информацию в сводной и детальной таблицах отчета.

    Ожидаемый результат: в отчете зафиксирована корректная информация об обнаружении зараженного файла (время события, путь к файлу, имя виртуальной машины).

kaspersky

О правах доступа к функциям программы

Доступ к функциям программы Kaspersky Security предоставляется пользователю в соответствии с его правами доступа к Серверу администрирования Kaspersky Security Center и его объектам.

1. Права на управление всеми параметрами программы Kaspersky Security и права на изменение конфигурации SVM предоставляются следующим пользователям:

   - администраторам Kaspersky Security Center (пользователям, входящим в группу KLAdmins);
   - локальным администраторам устройств, на которых установлен Сервер администрирования Kaspersky Security Center.

   Права на управление параметрами программы в рамках одного виртуального Сервера администрирования Kaspersky Security Center предоставляются администраторам этого виртуального Сервера администрирования.

   Для пользователей, которые не относятся к одной из этих категорий, доступ к функциям программы Kaspersky Security ограничен или запрещен.

   Подробную информацию об управлении правами доступа к Серверу администрирования Kaspersky Security Center и его объектам см. в документации Kaspersky Security Center.

2. Права на установку, удаление и обновление программы предоставляются пользователям VMware NSX Manager с ролью Enterprise Administrator.
3. Локальный пользователь защищаемой виртуальной машины не имеет прав доступа к функциям и управлению программой Kaspersky Security.

kaspersky

Защита виртуальных машин от файловых угроз

SVM с установленным компонентом Защита от файловых угроз обеспечивает защиту виртуальных машин на гипервизоре VMware ESXi. Параметры, которые SVM применяют во время защиты виртуальных машин от файловых угроз, задаются с помощью политик (см. раздел "О политиках Kaspersky Security" на стр. 18). Kaspersky Security начинает защищать виртуальные машины только после того, как вы включили защиту с помощью политики (см. раздел "Подготовка программы к работе. Включение защиты виртуальных машин" на стр. 65).

Защита виртуальных машин от файловых угроз включена, если этим виртуальным машинами назначен профиль защиты (см. раздел "О профилях защиты Kaspersky Security" на стр. 20). Вы можете назначить основной профиль защиты, который формируется автоматически при создании политики, или создать и назначить дополнительные профили защиты, если вы хотите использовать разные параметры защиты для разных объектов виртуальной инфраструктуры.

Вы можете назначать профили защиты непосредственно виртуальным машинам и другим объектам виртуальной инфраструктуры (см. раздел "Назначение профилей защиты объектам виртуальной инфраструктуры" на стр. 96). В виртуальной инфраструктуре под управлением автономного сервера VMware vCenter Server вы также можете назначать разные профили защиты виртуальным машинам в составе групп безопасности NSX (NSX Security Group), которые находятся под действием разных конфигураций профилей NSX (NSX Profile Configurations) (см. раздел "Назначение профилей защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)" на стр. 97).

Если на SVM программа не активирована (см. раздел "Процедура активации программы" на стр. 68) или отсутствуют базы программы (см. раздел "Процедура обновления баз программы" на стр. 69), Kaspersky Security не защищает виртуальные машины.

Kaspersky Security защищает виртуальные машины, для которых выполняются следующие условия:

- Виртуальная машина не выключена и не приостановлена.

  При выполнении задач проверки Kaspersky Security может проверять выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS.

- На виртуальной машине установлен и запущен драйвер Guest Introspection (NSX File Introspection Driver).
- Виртуальная машина входит в состав группы безопасности NSX (NSX Security Group), настроенной в консоли VMware vSphere Web Client. Для этой группы должна быть назначена политика безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).
- На виртуальную машину распространяется действие какого-либо профиля защиты.

Если хотя бы одно из перечисленных условий не выполняется, программа Kaspersky Security не защищает виртуальную машину.

Когда пользователь или программа обращается к файлу виртуальной машины, программа Kaspersky

Security проверяет этот файл.

- Если в файле не обнаружены вирусы или другие программы, представляющие угрозу, Kaspersky Security разрешает доступ к этому файлу.
- Если в файле обнаружены вирусы или другие программы, представляющие угрозу, Kaspersky Security присваивает файлу статус *Зараженный*. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или другим программам, представляющим угрозу, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус *Зараженный*.

  После этого Kaspersky Security выполняет над файлом то действие, которое указано в профиле защиты этой виртуальной машины, например лечит или блокирует файл.

Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из защиты. Список исключений настраивается в параметрах профилей защиты.

Во время защиты виртуальных машин используется метод проверки *Сигнатурный анализ и машинное обучение*. Защита с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. Kaspersky Security использует базы программы, содержащие информацию об известных угрозах и о методах их устранения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Сигнатурный анализ и машинное обучение всегда включен.

Также во время защиты виртуальных машин используется *эвристический анализ* – это технология обнаружения угроз, которые невозможно определить с помощью баз программ "Лаборатории Касперского". Эвристический анализ позволяет находить файлы, которые, возможно, содержат вредоносную программу, не указанную в базах, или новую модификацию известного вируса. Файлам, в которых во время эвристического анализа обнаружена угроза, присваивается статус *Зараженный*.

Уровень эвристического анализа зависит от выбранного уровня безопасности:

- Если установлен уровень безопасности **Низкий**, применяется поверхностный уровень эвристического анализа. Эвристический анализатор выполняет не все инструкции исполняемых файлов во время проверки исполняемых файлов на наличие вредоносного кода. При таком уровне эвристического анализа вероятность обнаружить угрозу снижена по сравнению со средним уровнем эвристического анализа. Проверка требует меньше ресурсов SVM и проходит быстрее.
- Если установлен уровень безопасности **Рекомендуемый**, **Высокий** или **Пользовательский**, применяется средний уровень эвристического анализа. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет то количество инструкций в исполняемых файлах, которое рекомендовано специалистами "Лаборатории Касперского".

Информация обо всех событиях, произошедших во время защиты виртуальных машин, передается на Сервер администрирования Kaspersky Security Center.

Рекомендуется периодически просматривать список файлов, заблокированных в результате защиты виртуальных машин, и выполнять действия с этими файлами. Например, вы можете сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Информацию о заблокированных файлах вы можете просмотреть в отчете о вирусах или в выборке событий по событию *Файл заблокирован* (см. в документации Kaspersky Security Center).

Чтобы получить доступ к файлам, заблокированным в результате защиты виртуальных машин, требуется исключить эти файлы из защиты в параметрах профиля, назначенного виртуальным машинам, или

временно выключить защиту этих виртуальных машин (см. раздел "Выключение защиты объектов виртуальной инфраструктуры от файловых угроз" на стр. 99).

В этом разделе

Настройка параметров основного профиля защиты

Основной профиль защиты автоматически формируется во время создания основной политики и политики для клиентов. Вы можете настроить параметры основного профиля защиты как во время создания политики (шаг **Настройка параметров основного профиля защиты**), так и в свойствах политики после ее создания (подраздел **Основной профиль защиты** в разделе **Защита от файловых угроз**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры основного профиля защиты, выполните следующие действия:*

1. В блоке **Уровень безопасности** выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины:
   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка**. В открывшемся окне **Параметры уровня безопасности** выполните следующие действия:

a. В блоке **Проверка архивов и составных файлов** укажите значения следующих параметров:

- **Проверять архивы**

  Включение / выключение проверки архивов.

  По умолчанию флажок снят.

- **Удалять архивы, если лечение не удалось**

  Включение / выключение функции удаления архивов, лечение которых невозможно.

  Если флажок установлен, Kaspersky Security удаляет архивы, которые не удалось вылечить.

  Если флажок снят, программа не удаляет невылеченные архивы. Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию о том, что зараженный файл не удален.

  Флажок доступен для изменения, если установлен флажок **Проверять архивы**.

  По умолчанию флажок снят.

- **Проверять самораспаковывающиеся архивы**

  Включение / выключение проверки самораспаковывающихся архивов.

  По умолчанию для профилей защиты флажок снят, для задач проверки флажок установлен.

- **Проверять вложенные OLE-объекты**

  Включение / выключение проверки объектов, вложенных в файл.

  По умолчанию флажок установлен.

- **Не распаковывать составные файлы большого размера**

  Если флажок установлен, Kaspersky Security не проверяет составные файлы, размер которых превышает значение поля **Максимальный размер проверяемого составного файла N МБ**.

  Если флажок снят, Kaspersky Security проверяет составные файлы любого размера.

  Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

  По умолчанию флажок установлен.

- **Максимальный размер проверяемого составного файла N МБ**

  Максимальный размер составных файлов, подлежащих проверке (в мегабайтах). Kaspersky Security не распаковывает и не проверяет те объекты, размер которых больше указанного значения.

  Параметр доступен для изменения, если установлен флажок **Не распаковывать составные файлы большого размера**.

  Вы можете указать в этом поле значение от 1 до 999999. По умолчанию задано значение 8 МБ.

b. В блоке **Производительность** укажите значения следующих параметров:

- **Ограничивать время проверки файлов**

  Включение / выключение ограничения времени проверки файлов.

  Если флажок установлен, Kaspersky Security прекращает проверку файла, если время проверки достигает значения, заданного в поле **Проверять файлы не дольше N секунд(ы)**, и пропускает этот файл.

  Если флажок снят, Kaspersky Security не ограничивает время проверки файлов.

  По умолчанию для профилей защиты флажок установлен, для задач проверки флажок снят.

- **Проверять файлы не дольше N секунд(ы)**

  Максимальная длительность проверки файла (в секундах). Kaspersky Security прекращает проверку файла, если она длится больше заданного значения времени.

  Параметр доступен для изменения, если установлен флажок **Ограничивать время проверки файлов**.

  Вы можете указать в этом поле значение от 1 до 3600. По умолчанию задано значение 60 секунд.

c. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка** и укажите в открывшемся окне **Объекты для обнаружения** значения следующих параметров:

- **Вредоносные утилиты**

  Включение / выключение защиты от вредоносных утилит.

  Вредоносные утилиты не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на виртуальной машине. Злоумышленники используют функции вредоносных утилит для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы или других вредоносных действий.

  Если флажок установлен, защита от вредоносных утилит включена.

  Если флажок снят, защита от вредоносных утилит выключена.

  По умолчанию флажок установлен.

- **Программы автодозвона**

  Включение / выключение защиты от программ автодозвона.

  Если флажок установлен, защита от программ автодозвона включена.

  Если флажок снят, защита от программ автодозвона выключена.

  По умолчанию флажок установлен.

- **Рекламные программы**

  Включение / выключение защиты от рекламных программ.

  Рекламные программы связаны с показом пользователю рекламной информации, например: отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-сайты. Некоторые из рекламных программ собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов рекламные программы передают эту информацию разработчику с разрешения пользователя.

  Если флажок установлен, защита от рекламных программ включена.

Если флажок снят, защита от рекламных программ выключена.

По умолчанию флажок установлен.

- **Другие**

  Включение / выключение защиты от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя.

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ находятся IRC-клиенты, программы для загрузки файлов, программы удаленного администрирования, программы для отслеживания действий пользователя, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet. Однако если злоумышленники получат доступ к таким программам, они могут использовать некоторые их функции для нанесения вреда виртуальной машине или данным пользователя.

  Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя, включена.

  Если флажок снят, защита от таких программ выключена.

  По умолчанию флажок снят.

- **Многократно упакованные файлы**

  Включение / выключение проверки файлов, которые упакованы одним или несколькими упаковщиками три или более раз.

  Если файл упакован одним или несколькими упаковщиками три или более раз, то существует вероятность, что файл содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Если флажок установлен, защита от многократно упакованных файлов включена, и проверка таких файлов разрешена.

  Если флажок снят, защита от многократно упакованных файлов выключена.

  По умолчанию флажок установлен.

  > Kaspersky Security всегда проверяет файлы виртуальных машин на наличие вирусов, червей и троянских программ. Поэтому параметры **Вирусы и черви** и **Троянские программы** в блоке **Вредоносные программы** недоступны для изменения.

d. Нажмите на кнопку **ОК** в окне **Объекты для обнаружения**.

e. Нажмите на кнопку **ОК** в окне **Параметры уровня безопасности**.

   Если вы изменили параметры уровня безопасности, программа создаст пользовательский уровень безопасности. Название уровня безопасности в блоке **Уровень безопасности** изменится на **Пользовательский**.

2. В блоке **Действие при обнаружении угрозы** выберите действие в раскрывающемся списке.

   Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов:

   - **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security

автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.

- **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

  Это действие выбрано по умолчанию.

  Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить, только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.

- **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.

- **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

3. Если вы хотите, чтобы во время защиты виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяла файлы на сетевых дисках, снимите флажок **Проверять сетевые диски** в блоке **Область защиты**. По умолчанию во время защиты виртуальных машин с операционными системами Windows программа проверяет на сетевых дисках все файлы, для которых не настроено исключение из защиты.

   Во время защиты виртуальных машин с операционными системами Linux программа Kaspersky Security всегда проверяет файлы поддерживаемых сетевых файловых систем (NFS и CIFS). Если вы хотите исключить из области защиты файлы сетевых файловых систем, вам требуется настроить исключение из защиты для директории, в которую смонтирована сетевая файловая система.

   > Kaspersky Security всегда проверяет файлы на съемных и жестких дисках. Поэтому параметр **Проверять все съемные и жесткие диски** в блоке **Область защиты** недоступен для изменения.

4. Если вы хотите исключить из защиты какие-либо файлы виртуальных машин, нажмите на кнопку **Настройка** в блоке **Исключения из защиты**.

   В открывшемся окне **Исключения из защиты** укажите следующие параметры:

   a. В блоке **Расширения файлов** выберите один из следующих вариантов:

      - **Проверять все, кроме файлов со следующими расширениями**. В поле ввода укажите список расширений файлов, которые не надо проверять во время защиты виртуальной машины. Kaspersky Security не учитывает регистр символов в расширениях файлов, которые требуется исключить из области защиты.

      - **Проверять только файлы со следующими расширениями**. В поле ввода укажите список расширений файлов, которые надо проверять во время защиты виртуальной машины. Во время защиты виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в расширениях файлов, которые требуется включить в область защиты. Во время защиты виртуальных машин с операционными системами Windows регистр символов в расширениях файлов не учитывается.

   Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении

используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

> Если вы выбрали в раскрывающемся списке вариант **Проверять только файлы со следующими расширениями**, но не указали расширения файлов, которые надо проверять, Kaspersky Security проверяет все файлы.

b. В таблице **Папки и файлы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список объектов, которые требуется исключить из защиты.

По умолчанию список исключений содержит объекты, рекомендуемые корпорацией Microsoft (список рекомендуемых исключений см. на сайте корпорации Microsoft). Kaspersky Security исключает эти объекты из защиты на всех виртуальных машинах, которым назначен основной профиль защиты. Вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы**.

Вы можете исключать из защиты объекты следующих типов:

- Папки. Из защиты исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение из защиты к вложенным папкам.
- Файлы по маске. Из защиты исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

  При указании маски файла вы можете использовать символы `*` и `?`.

Программа Kaspersky Security игнорирует регистр символов в путях к файлам и папкам, исключаемым из защиты.

Вы можете сохранить настроенный список исключений в файле с помощью кнопки **Экспорт** и загрузить ранее сохраненный список исключений из файла с помощью кнопки **Импорт**. Для импорта и экспорта списка исключений вы можете использовать файл в формате XML. Импортировать список исключений вы также можете из файла в формате DAT. С помощью файла в формате DAT вы можете импортировать список исключений, сформированный в других программах "Лаборатории Касперского".

> Если вы используете в списке исключений переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows из защиты исключаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, из защиты исключаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

5. Нажмите на кнопку **ОК** в окне **Исключения из защиты**.
6. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания политики) или на кнопку **Применить** (в свойствах политики).

Измененные параметры профиля защиты вступят в силу после синхронизации данных между программой Kaspersky Security Center и SVM.

kaspersky

Управление дополнительными профилями защиты

Вы можете управлять дополнительными профилями защиты в свойствах политики в списке дополнительных профилей защиты.

► *Чтобы открыть список дополнительных профилей защиты в свойствах политики, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики в разделе **Защита от файловых угроз** выберите подраздел **Дополнительные профили защиты**.

   В правой части окна отобразится список дополнительных профилей защиты. Если вы еще не создавали дополнительные профили защиты в этой политике, то список профилей защиты пуст.

В списке дополнительных профилей защиты вы можете выполнять следующие действия:

- Создавать дополнительные профили защиты (см. раздел "Создание дополнительного профиля защиты" на стр. 92).
- Изменять имя дополнительного профиля защиты по кнопке **Переименовать**.
- Изменять параметры дополнительного профиля защиты по кнопке **Изменить**. Изменение параметров выполняется в окне **Параметры защиты**. Параметры дополнительного профиля защиты аналогичны параметрам основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 85). Измененные параметры профиля защиты вступают в силу после синхронизации данных между программой Kaspersky Security Center и SVM.
- Экспортировать параметры дополнительного профиля защиты в файл по кнопке **Экспорт**. Для сохранения параметров дополнительного профиля защиты нужно указать путь к файлу в формате JSON. Ранее сохраненные параметры вы можете использовать при создании нового дополнительного профиля защиты.
- Удалять дополнительный профиль защиты по кнопке **Удалить**. Если этот профиль защиты использовался для защиты виртуальных машин, программа будет защищать эти виртуальные машины с параметрами профиля защиты, который назначен их родительскому объекту в виртуальной инфраструктуре. Если родительский объект исключен из защиты, программа не будет защищать эти виртуальные машины.

  Если параметры файловой защиты заданы с использованием конфигураций профилей NSX (NSX Profile Configurations), при удалении профиля защиты будет отменено соответствие между удаленным профилем защиты и конфигурацией профиля NSX. Программа будет защищать виртуальные машины, на которые распространяется действие этой конфигурации профиля NSX, с параметрами профиля защиты по умолчанию.

kaspersky

Создание дополнительного профиля защиты

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы создать дополнительный профиль защиты, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте список дополнительных профилей защиты в свойствах политики, для которой вы хотите создать дополнительный профиль защиты (см. раздел "Управление дополнительными профилями защиты" на стр. 91).
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Профиль защиты**.
3. В открывшемся окне введите имя нового профиля защиты.

   Имя профиля защиты не может содержать более 255 символов.
4. Если при создании нового профиля защиты вы хотите использовать ранее сохраненные параметры профиля защиты (см. раздел "Управление дополнительными профилями защиты" на стр. 91), установите флажок **Импортировать параметры из файла** и укажите путь к файлу в формате JSON.
5. Нажмите на кнопку **ОК** в окне **Профиль защиты**.

   Откроется окно **Параметры защиты**. В этом окне вы можете настроить параметры нового профиля защиты или изменить параметры профиля защиты, импортированные из файла.

   Параметры дополнительного профиля защиты, кроме списка исключений по умолчанию, аналогичны параметрам основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 85).

   Список исключений по умолчанию не содержит объекты, рекомендуемые корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Если вы хотите, чтобы объекты, рекомендуемые корпорацией Microsoft, исключались из защиты на всех виртуальных машинах, которым назначен этот профиль защиты, вам нужно импортировать в исключения профиля защиты файл microsoft_file_exclusions.xml.
   Файл microsoft_file_exclusions.xml входит в комплект поставки программы и расположен в папке установки плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. После импортирования вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы** в окне **Исключения из защиты**.
6. После настройки всех параметров профиля защиты нажмите на кнопку **ОК** в окне **Параметры защиты**.

В окне **Свойства: <Название политики>** в списке дополнительных профилей защиты отобразится новый профиль защиты.

Созданные дополнительные профили вы можете назначать виртуальным машинам или другим объектам виртуальной инфраструктуры VMware (см. раздел "Назначение профилей защиты объектам виртуальной инфраструктуры" на стр. 96), а также устанавливать соответствия между профилями защиты и конфигурациями профилей NSX (NSX Profile Configurations) (см. раздел "Назначение профилей защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)" на стр. 97).

Просмотр защищаемой инфраструктуры в политике

В свойствах политики вы можете посмотреть защищаемую инфраструктуру, выбранную для политики, и информацию об использовании профилей защиты.

► *Чтобы просмотреть информацию о защищаемой инфраструктуре в политике, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики в разделе **Защита от файловых угроз** выберите подраздел **Защищаемая инфраструктура**.
3. Плагин управления Kaspersky Security пытается автоматически подключиться к Серверу интеграции. Если установить подключение не удалось, откроется окно **Подключение к Серверу интеграции**.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции по умолчанию используется ваша доменная учетная запись. Флажок **Использовать доменную учетную запись** установлен по умолчанию. Вы также можете использовать учетную запись администратора Сервера интеграции (admin). Для этого снимите флажок **Использовать доменную учетную запись** и введите пароль администратора в поле **Пароль**.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или компьютер входит в домен, но ваша доменная учетная запись не входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции вы можете использовать только учетную запись администратора Сервера интеграции (admin). Введите пароль администратора в поле **Пароль**.

   Если для подключения к Серверу интеграции вы используете учетную запись администратора Сервера интеграции (admin), вы можете сохранить пароль администратора. Для этого установите флажок **Сохранить пароль**. При следующем подключении к этому Серверу интеграции используется сохраненный пароль администратора. Если вы снимаете флажок, установленный при предыдущем подключении к Серверу интеграции, Kaspersky Security удаляет ранее сохраненный пароль администратора Сервера интеграции.

   Флажок **Сохранить пароль** может быть недоступен, если на компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, установлены обновления Windows KB

2992611 и / или KB 3000850. Чтобы восстановить возможность сохранения пароля администратора, вы можете удалить эти обновления Windows или внести изменения в реестр операционной системы, как описано в Базе знаний https://support.kaspersky.ru/15285.

Укажите параметры подключения и нажмите на кнопку **ОК** в окне **Подключение к Серверу интеграции**.

4. Плагин управления Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

   Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

После подключения к Серверу интеграции в правой части окна отображается информация о защищаемой инфраструктуре и использовании профилей защиты.

В свойствах основной политики, которая определяет параметры защиты виртуальной инфраструктуры под управлением одного сервера VMware vCenter Server, вы можете выбрать способ назначения параметров файловой защиты в раскрывающемся списке, расположенном в верхней части окна:

- **Использовать дерево виртуальной инфраструктуры**. Если выбран этот вариант, в таблице отображается дерево объектов виртуальной инфраструктуры VMware и профили защиты, назначенные объектам виртуальной инфраструктуры.
- **Использовать конфигурации профилей NSX (NSX Profile Configurations)**. Если выбран этот вариант, в таблице отображаются конфигурации профилей NSX (NSX Profile Configurations), доступные для выбранного сервера VMware vCenter Server, и соответствующие им профили защиты.

Если в качестве защищаемой инфраструктуры для политики выбрана вся защищаемая инфраструктура, назначение параметров файловой защиты с использованием конфигураций профилей NSX недоступно. В раскрывающемся списке выбран вариант **Использовать дерево виртуальной инфраструктуры**.

Информация о назначении параметров файловой защиты с использованием дерева виртуальной инфраструктуры

Если в раскрывающемся списке, расположенном в верхней части окна, выбран вариант **Использовать дерево виртуальной инфраструктуры**, в разделе **Защищаемая инфраструктура** отображаются дерево объектов виртуальной инфраструктуры VMware и профили защиты, назначенные объектам виртуальной инфраструктуры.

Защищаемая инфраструктура отображается в виде дерева элементов:

- В свойствах политики для одного сервера VMware vCenter Server отображается защищаемая инфраструктура кластера "VMware vCenter Agentless": корневым элементом является сервер VMware vCenter Server, под ним расположены объекты Datacenter, кластеры VMware, ресурсные пулы, объекты vApp и виртуальные машины.
- В свойствах политики для всей защищаемой инфраструктуры корневым элементом является Сервер интеграции, под ним расположены все серверы VMware vCenter Server, каждый из них содержит защищаемую инфраструктуру кластера "VMware vCenter Agentless", соответствующего этому серверу VMware vCenter Server.
- В свойствах политики для клиентов, размещенной в папке **Управляемые устройства** виртуального Сервера администрирования, корневым элементом является условный объект "Организация vCloud Director", который объединяет все виртуальные Datacenter клиента. Под ним расположены все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования.

Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если этой виртуальной машине назначен профиль защиты, параметры этого профиля защиты применяются ко всем виртуальным машинам, которые имеют одинаковый идентификатор (vmID).

В графе **Профиль защиты** отображается информация о назначении объектам защищаемой инфраструктуры профилей защиты. Параметры назначенных профилей защиты Kaspersky Security использует во время защиты виртуальных машин.

Графа **Профиль защиты** может содержать следующие значения:

- Имя профиля защиты, назначенного виртуальной машине или объекту виртуальной инфраструктуры VMware.
- Имя профиля защиты, унаследованного от родительского объекта, в виде "унаследованный: <N>", где <N> – имя унаследованного профиля защиты.
- *(Не назначен)* или *унаследованный: (Не назначен)* – если профиль защиты не назначался или назначение профиля защиты было отменено (выбрано значение **Не использовать профиль защиты**). Виртуальные машины или объекты виртуальной инфраструктуры, которым не назначен профиль защиты, исключаются из защиты.

Информация о назначении параметров файловой защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)

Если в раскрывающемся списке, расположенном в верхней части окна, выбран вариант **Использовать конфигурации профилей NSX (NSX Profile Configurations)**, в разделе **Защищаемая инфраструктура** отображаются следующие сведения:

- Имя профиля защиты по умолчанию. Этот профиль защиты соответствует конфигурациям профилей NSX, для которых соответствие с профилем защиты еще не устанавливалось, или соответствие было отменено в результате удаления профиля защиты.

  В качестве профиля защиты по умолчанию выбран основной профиль защиты. Если вы отменили использование профиля защиты по умолчанию, в строке отображается значение *Не использовать профиль защиты*.
- Таблица соответствий между конфигурациями профилей NSX, доступными для выбранного сервера VMware vCenter Server, и профилями защиты.

В таблице отображаются следующие сведения:

- Графа **Конфигурация профиля NSX** содержит имя конфигурации профиля NSX (NSX Profile Configuration). Если в виртуальной инфраструктуре создано несколько конфигураций профилей NSX с одинаковым идентификатором (Configuration ID), их имена отображаются через запятую. Конфигурации профилей NSX с одинаковыми идентификаторами программа Kaspersky Security обрабатывает как одну и ту же конфигурацию профиля NSX.
- Если соответствие между конфигурацией профиля NSX и профилем защиты установлено, в графе **Профиль защиты** отображается имя профиля защиты. Для защиты виртуальных машин, на которые распространяется действие этой конфигурации профиля NSX, Kaspersky Security использует параметры указанного профиля защиты.
- Если соответствие было отменено, в графе **Профиль защиты** отображается значение *(Не назначен)*. Если конфигурации профиля NSX не соответствует никакой профиль защиты, виртуальные машины, на которые распространяется действие этой конфигурации профиля NSX, исключаются из защиты.

Назначение профилей защиты объектам виртуальной инфраструктуры

► *Чтобы назначить виртуальной машине или другому объекту виртуальной инфраструктуры VMware профиль защиты, выполните следующие действия:*

1. В свойствах политики, в области действия которой находятся нужные виртуальные машины или другие объекты виртуальной инфраструктуры VMware, выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. Если вы настраиваете политику для одного сервера VMware vCenter Server, убедитесь, что в раскрывающемся списке, расположенном в верхней части окна, выбран вариант **Использовать дерево виртуальной инфраструктуры**. Это значение выбрано по умолчанию.
3. Выберите один или несколько объектов виртуальной инфраструктуры в таблице.

   Если вы хотите назначить одинаковый профиль защиты нескольким виртуальным машинам, которые являются дочерними объектами одного объекта виртуальной инфраструктуры, выберите в таблице этот объект. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.
4. Нажмите на кнопку **Выбрать профиль защиты**.

   Откроется окно **Выбор профиля защиты**.
5. Выберите один из следующих вариантов:
   - **Наследовать родительский профиль защиты: <имя>**. Выберите этот вариант, чтобы назначить виртуальной машине или другому объекту виртуальной инфраструктуры профиль защиты родительского объекта.
   - **Использовать профиль защиты**. Выберите этот вариант и укажите в раскрывающемся списке имя профиля защиты, чтобы назначить этот профиль защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.
6. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, профиль защиты назначается объекту и всем его дочерним объектам, включая объекты, которым назначен собственный профиль защиты или которые исключены из защиты. Если вы хотите назначить профиль защиты только выбранному объекту виртуальной инфраструктуры и тем его дочерним объектам,

которым не назначен собственный профиль защиты и которые не исключены из защиты, снимите флажок **Применить ко всем дочерним объектам**.

7. Нажмите на кнопку **ОК**.

   Окно **Выбор профиля защиты** закроется, назначенный профиль защиты отобразится в таблице в подразделе **Защищаемая инфраструктура**.

8. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Назначение профилей защиты с использованием конфигураций профилей NSX (NSX Profile Configurations)

В виртуальной инфраструктуре под управлением автономного сервера VMware vCenter Server программа Kaspersky Security позволяет задавать параметры файловой защиты на уровне групп безопасности NSX (NSX Security Group). Вы можете назначить одинаковые параметры файловой защиты всем виртуальным машинам, входящим в одну группу безопасности NSX. Для этого вам нужно распределить виртуальные машины по группам безопасности NSX и для каждой группы безопасности выполнить следующие действия:

1. В консоли VMware vSphere Web Client:

   a. Создать конфигурацию профиля NSX (NSX Profile Configuration). Чтобы запустить мастер создания конфигурации профиля NSX, вам нужно открыть свойства службы Kaspersky File Antimalware Protection (раздел **Networking & Security** → **Service Definitions**, закладка **Services**, действие **Edit Settings**) и перейти на закладку **Manage** → **Profile Configurations**.

   b. Указать эту конфигурацию профиля NSX или профиль службы NSX (NSX Service Profile), созданный на основе этой конфигурации профиля NSX, в политике безопасности NSX (NSX Security Policy).

   c. Назначить политику безопасности NSX на группу безопасности NSX (NSX Security Group).

2. В Консоли администрирования Kaspersky Security Center в свойствах политики Kaspersky Security установить соответствие между конфигурацией профиля NSX и профилем защиты.

   Параметры профиля защиты будут использоваться во время защиты виртуальных машин из группы безопасности NSX, на которую применена политика безопасности NSX.

► *Чтобы установить соответствие между конфигурацией профиля NSX и профилем защиты, выполните следующие действия:*

1. В свойствах политики для одного сервера VMware vCenter Server выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант **Использовать конфигурации профилей NSX (NSX Profile Configurations)**.
3. В таблице выберите конфигурацию профиля NSX, для которой вы хотите установить соответствие, и двойным щелчком мыши откройте окно **Выбор профиля защиты**.
4. В открывшемся окне выберите вариант **Использовать профиль защиты** и в раскрывающемся списке укажите имя профиля защиты, который должен соответствовать конфигурации профиля NSX. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.
5. Нажмите на кнопку **ОК**.

Окно **Выбор профиля защиты** закроется, установленное соответствие отобразится в таблице в подразделе **Защищаемая инфраструктура**.

6. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Конфигурациям профилей NSX, для которых еще не устанавливалось соответствие с профилем защиты, или соответствие было отменено в результате удаления профиля защиты, автоматически назначается профиль защиты по умолчанию. Вы можете изменить профиль защиты по умолчанию или отменить использование профиля защиты по умолчанию.

► *Чтобы изменить профиль защиты по умолчанию, выполните следующие действия:*

1. В свойствах политики для одного сервера VMware vCenter Server выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант **Использовать конфигурации профилей NSX (NSX Profile Configurations)**.
3. Нажмите на кнопку **Изменить**, расположенную справа от названия профиля защиты по умолчанию.

   Откроется окно **Выбор профиля защиты**.
4. Если вы хотите изменить профиль защиты по умолчанию, выберите вариант **Использовать профиль защиты** и укажите в раскрывающемся списке имя профиля защиты. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.

   Указанный профиль защиты будет соответствовать конфигурациям профилей NSX, для которых соответствие с профилем защиты еще не устанавливалось, или соответствие было отменено в результате удаления профиля защиты.
5. Если вы хотите отменить использование профиля защиты по умолчанию, выберите вариант **Не использовать профиль защиты**. Конфигурациям профилей NSX, для которых соответствие с профилем защиты еще не устанавливалось, или соответствие было отменено в результате удаления профиля защиты, по умолчанию не будет соответствовать никакой профиль защиты. Виртуальные машины, находящиеся под действием этих конфигураций профилей NSX, будут исключены из защиты.
6. Нажмите на кнопку **ОК**.

   Окно **Выбор профиля защиты** закроется, в верхней части окна в подразделе **Защищаемая инфраструктура** отобразится имя выбранного профиля защиты.
7. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Изменение защищаемой инфраструктуры для политики

Вы можете изменить защищаемую инфраструктуру, выбранную для политики. Это может потребоваться, например, если вы хотите скопировать политику из одной группы администрирования в другую. В этом случае вам нужно изменить для скопированной политики защищаемую инфраструктуру так, чтобы защищаемая инфраструктура соответствовала расположению политики:

- если политика расположена в группе, которая содержит кластер "VMware vCenter Agentless", в качестве защищаемой инфраструктуры для политики должен быть выбран сервер VMware vCenter Server, соответствующий этому кластеру;
- если политика расположена в папке **Управляемые устройства** или в группе, которая содержит кластер "VMware vCloud Director Agentless", в качестве защищаемой инфраструктуры для политики должна быть выбрана вся защищаемая инфраструктура.

► *Чтобы изменить защищаемую инфраструктуру, выбранную для политики, выполните следующие действия:*

1. В свойствах политики, защищаемую инфраструктуру которой вы хотите изменить, выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. В правой части окна нажмите на кнопку **Изменить**.
3. Откроется окно **Подключение к Серверу интеграции**. В окне отображаются параметры подключения к тому Серверу интеграции, адрес которого указан в нижней части окна в подразделе **Защищаемая инфраструктура**. Если требуется, измените параметры подключения и нажмите на кнопку **ОК**.
4. После того, как подключение будет установлено, откроется окно **Выбор защищаемой инфраструктуры**. Выберите один из следующих вариантов:
   - Если вы настраиваете политику, расположенную в группе администрирования, которая содержит кластер "VMware vCenter Agentless", выберите вариант **Один сервер VMware vCenter Server**. Затем выберите в списке сервер VMware vCenter Server, соответствующий этому кластеру "VMware vCenter Agentless".

     Если выбранный VMware vCenter Server не соответствует кластеру "VMware vCenter Agentless", в группе которого расположена политика, Kaspersky Security не защищает виртуальные машины.

   - Если вы настраиваете политику, расположенную в любой другой папке или группе администрирования, выберите вариант **Вся защищаемая инфраструктура**.
5. Нажмите на кнопку **ОК** в окне **Выбор защищаемой инфраструктуры** и подтвердите в открывшемся окне изменение защищаемой инфраструктуры.
6. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Выключение защиты объектов виртуальной инфраструктуры от файловых угроз

Выключение функции защиты приводит к выходу программы из сертифицированного состояния.

Вы можете выключить защиту объектов виртуальной инфраструктуры от файловых угроз следующими способами:

- Если параметры файловой защиты заданы путем назначения профилей защиты объектам виртуальной инфраструктуры, вы можете отменить назначение профиля защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Виртуальные машины, которым не назначен профиль защиты, исключаются из защиты.
- Если параметры файловой защиты заданы с использованием конфигураций профилей NSX (NSX Profile Configurations), вы можете отменить соответствие между профилем защиты и конфигурацией профиля NSX, действие которой распространяется на виртуальные машины. Если конфигурации профиля NSX не соответствует никакой профиль защиты, виртуальные машины, на которые распространяется действие этой конфигурации профиля NSX, исключаются из защиты.

- Вы можете выключить защиту для всех виртуальных машин, которые находятся в области действия политики.

► *Если параметры файловой защиты заданы путем назначения профилей защиты объектам виртуальной инфраструктуры, чтобы выключить защиту для одной или нескольких виртуальных машин, выполните следующие действия:*

1. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. Если вы настраиваете политику для одного сервера VMware vCenter Server, убедитесь, что в раскрывающемся списке, расположенном в верхней части окна, выбран вариант **Использовать дерево виртуальной инфраструктуры**.
3. Выберите один или несколько объектов виртуальной инфраструктуры в графе **Имя**.

   Если вы хотите выключить защиту для нескольких виртуальных машин, которые являются дочерними объектами одного объекта виртуальной инфраструктуры, выберите этот объект. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.
4. Нажмите на кнопку **Выбрать профиль защиты**.

   Откроется окно **Выбор профиля защиты**.
5. Выберите вариант **Не использовать профиль защиты**.
6. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, по умолчанию защита будет выключена для выбранного объекта и для всех его дочерних объектов, включая объекты, которым назначен собственный профиль защиты. Если вы хотите выключить защиту только для выбранного объекта виртуальной инфраструктуры и тех его дочерних объектов, которые наследуют профиль защиты, снимите флажок **Применить ко всем дочерним объектам**.

   Защита будет снята с родительского объекта и тех его дочерних объектов, у которых профиль защиты унаследован от родительского объекта. Под защитой программы останутся дочерние объекты, которым назначен собственный профиль защиты.
7. Нажмите на кнопку **ОК**.

   Окно **Выбор профиля защиты** закроется, в таблице в подразделе **Защищаемая инфраструктура** для объектов, которые исключены из защиты, в графе **Профиль защиты** отобразится значение *(Не назначен)*.
8. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

► *Если параметры файловой защиты заданы с использованием конфигураций профилей NSX, чтобы выключить защиту виртуальных машин, выполните следующие действия:*

1. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант **Использовать конфигурации профилей NSX (NSX Profile Configurations)**.
3. В таблице выберите конфигурацию профиля NSX, действие которой распространяется на нужные виртуальные машины, и двойным щелчком мыши откройте окно **Выбор профиля защиты**.
4. В открывшемся окне выберите вариант **Не использовать профиль защиты**.

5. Нажмите на кнопку **ОК**.

   Окно **Выбор профиля защиты** закроется, в таблице в подразделе **Защищаемая инфраструктура** для выбранной конфигурации профиля NSX в графе **Профиль защиты** отобразится значение *(Не назначен)*.

6. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

► *Чтобы выключить защиту для всех виртуальных машин, которые находятся в области действия политики, выполните следующие действия:*

1. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 93).
2. Снимите флажок **Использовать защиту от файловых угроз**, расположенный в верхней части окна.
3. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

kaspersky

Проверка виртуальных машин

Kaspersky Security позволяет выполнять антивирусную проверку файлов виртуальных машин на гипервизоре VMware ESXi. Требуется периодически проверять файлы виртуальных машин с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов.

Kaspersky Security проверяет виртуальные машины, для которых выполняются следующие условия:

- Для выключенных виртуальных машин: на виртуальной машине используется файловая система NTFS, FAT32, EXT2, EXT3, EXT4, XFS или BTRFS.
- Для включенных виртуальных машин:
  - на виртуальной машине установлен и запущен драйвер Guest Introspection (NSX File Introspection Driver).
  - виртуальная машина входит в состав группы безопасности NSX (NSX Security Group), настроенной в консоли VMware vSphere Web Client. Для этой группы должна быть назначена политика безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

    Выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS программа Kaspersky Security может проверять в соответствии с параметрами проверки независимо от того, входят ли эти виртуальные машины в состав группы безопасности NSX (NSX Security Group).

Если хотя бы одно из перечисленных условий не выполняется, Kaspersky Security не проверяет виртуальную машину.

Kaspersky Security также не проверяет виртуальную машину, если выполняется одно из следующих условий:

- Вы добавили виртуальную машину в список объектов виртуальной инфраструктуры (Inventory) в консоли VMware vSphere Web Client или создали виртуальную машину на гипервизоре VMware ESXi после того, как была запущена задача проверки.
- Вы удалили виртуальную машину из списка объектов виртуальной инфраструктуры (Inventory) в консоли VMware vSphere Web Client до начала проверки этой виртуальной машины.
- Виртуальная машина, входящая в область действия запущенной задачи проверки, мигрирует на гипервизор VMware ESXi, на котором не запущена задача проверки.

Параметры, которые SVM применяют во время проверки виртуальных машин, задаются с помощью задач проверки. Kaspersky Security использует для проверки следующие задачи:

- **Полная проверка**. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин, находящихся в области действия задачи. Область действия задачи (см. раздел "Задачи проверки" на стр. 26) зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

  Задача полной проверки автоматически создается после установки основного плагина управления Kaspersky Security в папке **Управляемые устройства** главного Сервера администрирования Kaspersky Security Center. Эта задача позволяет выполнять антивирусную проверку всех виртуальных машин, которые находятся под защитой всех SVM и не входят в организации vCloud Director. Вы можете запускать эту задачу вручную.
- **Выборочная проверка**. Задача позволяет выполнять антивирусную проверку файлов указанных виртуальных машин из области действия задачи. Область действия задачи (см. раздел "Задачи

проверки" на стр. 26) зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу. В рамках выбранной области действия вам нужно указать виртуальные машины, которые требуется проверять. Вы можете указывать отдельные виртуальные машины, объекты виртуальной инфраструктуры VMware более высокого уровня иерархии или группы безопасности NSX (NSX Security Group), в которые входят нужные виртуальные машины.

Вы можете запускать задачи проверки вручную, задавать расписание выполнения задач проверки и просматривать информацию о ходе и результатах выполнения задач (см. раздел "О задачах Kaspersky Security" на стр. 24).

Если во время проверки файлов виртуальных машин в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус *Зараженный*. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус *Зараженный*.

При проверке виртуальных машин используется метод проверки *Сигнатурный анализ и машинное обучение*. Проверка с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. Kaspersky Security использует базы программы, содержащие информацию об известных угрозах и о методах их устранения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Сигнатурный анализ и машинное обучение всегда включен.

Также при проверке виртуальных машин используется *эвристический анализ* – это технология обнаружения угроз, которые невозможно определить с помощью баз программ "Лаборатории Касперского". Эвристический анализ позволяет находить файлы, которые, возможно, содержат вредоносную программу, не указанную в базах, или новую модификацию известного вируса. Файлам, в которых во время эвристического анализа обнаружена угроза, присваивается статус *Зараженный*.

Во время проверки виртуальных машин всегда используется глубокий уровень эвристического анализа независимо от выбранного уровня безопасности. Эвристический анализатор выполняет максимальное количество инструкций в исполняемых файлах, что позволяет повысить вероятность обнаружения угрозы.

Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из области проверки задачи.

Особенности проверки виртуальных машин:

- При выполнении задач проверки Kaspersky Security может проверять выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS.
- При выполнении задач проверки Kaspersky Security может проверять шаблоны виртуальных машин.
- При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется настроить задачу проверки для виртуальных машин, на которых открыт сетевой доступ к папкам и файлам, и включить эти папки и файлы в область проверки задачи.

  При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

- Во время выполнения задачи проверки одна SVM с установленным компонентом Защита от файловых угроз одновременно проверяет файлы не более четырех виртуальных машин.

Информация о результатах проверки и обо всех событиях, произошедших во время выполнения задачи проверки, передается на Сервер администрирования Kaspersky Security Center.

После завершения задачи проверки рекомендуется просмотреть список файлов, заблокированных в результате выполнения задачи, и вручную выполнить действия с этими файлами. Например, сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Предварительно требуется исключить заблокированные файлы из защиты в параметрах профиля, назначенного виртуальным машинам, или временно выключить защиту виртуальных машин, на которых были заблокированы эти файлы (см. раздел "Выключение защиты объектов виртуальной инфраструктуры от файловых угроз" на стр. 99). Информацию о заблокированных файлах вы можете просмотреть в отчете о вирусах или в выборке событий по событию *Файл заблокирован* (см. в документации Kaspersky Security Center).

В этом разделе

Создание задачи полной проверки

► *Чтобы создать задачу полной проверки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой вы хотите создать задачу (см. раздел "Задачи проверки" на стр. 26).

   Если вы выбрали папку **Управляемые устройства** или группу администрирования, содержащую кластер KSC, в рабочей области выберите закладку **Задачи**.

2. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
3. На первом шаге мастера выберите тип задачи.

   - Если вы хотите создать задачу для проверки виртуальных машин, которые не входят в организации vCloud Director, выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента → Полная проверка**.
   - Если вы хотите создать задачу для проверки виртуальных машин клиентов, выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов) → Полная проверка**.

   Перейдите к следующему шагу мастера создания задачи.
4. Настройте параметры проверки виртуальных машин (см. раздел "Настройка параметров проверки виртуальных машин в задаче проверки" на стр. 109).

   Перейдите к следующему шагу мастера создания задачи.

5. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи (см. раздел "Настройка области проверки в задаче проверки" на стр. 115).

   Перейдите к следующему шагу мастера создания задачи.

6. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM, на которых должна выполняться задача:

   - Нажмите на кнопку **Выбрать устройства, обнаруженные в сети Сервером администрирования**, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
   - Нажмите на кнопку **Задать адреса устройств вручную или импортировать из списка**, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

     Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

   - Нажмите на кнопку **Назначить задачу выборке устройств**, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.
   - Нажмите на кнопку **Назначить задачу группе администрирования**, если задача должна выполняться на всех SVM, входящих в группу администрирования.

     В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

     - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.
     - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM.
     - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
     - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
     - Нажмите на кнопку **Обзор** и выберите группу администрирования или введите название группы администрирования вручную.

   Перейдите к следующему шагу мастера создания задачи.

7. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач проверки" на стр. 119) и перейдите к следующему шагу мастера.
8. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера.
9. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

   Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

Создание задачи выборочной проверки с помощью основного плагина

Задача выборочной проверки, созданная с помощью основного плагина управления Kaspersky Security, позволяет проверять виртуальные машины, которые находятся под управлением одного сервера VMware vCenter Server и не входят в организации vCloud Director.

► *Чтобы создать задачу выборочной проверки для виртуальных машин, которые не входят в организации vCloud Director, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите группу администрирования, в которой вы хотите создать задачу (см. раздел "Задачи проверки" на стр. 26).

   В связи с особенностями настройки области действия задачи выборочной проверки рекомендуется создавать задачи выборочной проверки в группах администрирования, которые содержат кластеры KSC, то есть групповые задачи. Если задача выборочной проверки настроена для одной или нескольких SVM (то есть является локальной или глобальной задачей), не гарантируется возможность правильной настройки области действия задачи.

2. В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
3. На первом шаге мастера выберите тип задачи: **Kaspersky Security для виртуальных сред 6.0 Защита без агента** → **Выборочная проверка**.

   Перейдите к следующему шагу мастера создания задачи.
4. Мастер выполняет подключение к Серверу интеграции для получения информации о виртуальной инфраструктуре VMware.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции по умолчанию используется ваша доменная учетная запись. Флажок **Использовать доменную учетную запись** установлен по умолчанию.

   Если вы хотите использовать учетную запись администратора Сервера интеграции (admin), снимите флажок **Использовать доменную учетную запись** и введите пароль администратора в поле **Пароль**.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или компьютер входит в домен, но ваша доменная учетная запись не входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции вы можете использовать только учетную запись администратора Сервера интеграции (admin). Введите пароль администратора в поле **Пароль**.

   Если для подключения к Серверу интеграции вы используете учетную запись администратора Сервера интеграции (admin), вы можете сохранить пароль администратора. Для этого установите флажок **Сохранить пароль**. При следующем подключении к этому Серверу интеграции используется

сохраненный пароль администратора. Если вы снимаете флажок, установленный при предыдущем подключении к Серверу интеграции, Kaspersky Security удаляет ранее сохраненный пароль администратора Сервера интеграции.

Флажок **Сохранить пароль** может быть недоступен, если на компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, установлены обновления Windows KB 2992611 и / или KB 3000850. Чтобы восстановить возможность сохранения пароля администратора, вы можете удалить эти обновления Windows или внести изменения в реестр операционной системы, как описано в Базе знаний https://support.kaspersky.ru/15285.

Перейдите к следующему шагу мастера создания задачи.

Мастер создания задачи проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

После того, как подключение будет установлено, откроется окно **Список серверов VMware vCenter Server**. Выберите VMware vCenter Server, под управлением которого находятся виртуальные машины, которые вы хотите проверять, и нажмите на кнопку **ОК**.

5. На этом шаге мастера выберите область действия задачи (см. раздел "Настройка области действия задачи выборочной проверки" на стр. 118).

   Перейдите к следующему шагу мастера создания задачи.

6. Настройте параметры проверки виртуальных машин (см. раздел "Настройка параметров проверки виртуальных машин в задаче проверки" на стр. 109).

   Перейдите к следующему шагу мастера создания задачи.

7. Если требуется, сформируйте область проверки для задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи (см. раздел "Настройка области проверки в задаче проверки" на стр. 115).

   Перейдите к следующему шагу мастера создания задачи.

8. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач проверки" на стр. 119) и перейдите к следующему шагу мастера создания задачи.

9. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера создания задачи.

10. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

    Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

В случае замены / переустановки сервера VMware vCenter Server все ранее созданные задачи выборочной проверки перестают работать. Если вы хотите использовать ранее созданную задачу выборочной проверки, вам требуется выполнить повторное подключение к серверу VMware vCenter Server в свойствах этой задачи.

Создание задачи выборочной проверки с помощью плагина для клиентов

Задача выборочной проверки для виртуальных машин клиентов используется, только если программа работает в режиме multitenancy. Создание задачи выборочной проверки для виртуальных машин клиентов поддерживается только на виртуальном Сервере администрирования Kaspersky Security Center.

► *Чтобы создать задачу выборочной проверки для виртуальных машин клиентов, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства** виртуального Сервера администрирования, соответствующего клиенту.
2. В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
3. На первом шаге мастера выберите тип задачи: **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** → **Выборочная проверка**.

   Перейдите к следующему шагу мастера создания задачи.
4. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера создания задачи.

   Мастер создания задачи проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

   Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать**

предупреждения для <адрес Сервера интеграции>, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

5. Выберите область действия задачи: установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

   Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

   Перейдите к следующему шагу мастера создания задачи.

6. Настройте параметры проверки виртуальных машин (см. раздел "Настройка параметров проверки виртуальных машин в задаче проверки" на стр. 109).

   Перейдите к следующему шагу мастера создания задачи.

7. Если требуется, сформируйте область проверки для задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи (см. раздел "Настройка области проверки в задаче проверки" на стр. 115).

   Перейдите к следующему шагу мастера создания задачи.

8. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач проверки" на стр. 119) и перейдите к следующему шагу мастера создания задачи.

9. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера создания задачи.

10. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

    Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

Настройка параметров проверки виртуальных машин в задаче проверки

Вы можете настроить параметры проверки виртуальных машин во время создания задачи (шаг **Настройка параметров проверки**) или в свойствах задачи после ее создания (раздел **Параметры проверки**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры проверки виртуальных машин, выполните следующие действия:*

1. Выберите уровень безопасности, в соответствии с которым программа Kaspersky Security проверяет виртуальные машины. Для этого в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка**. В открывшемся окне **Параметры уровня безопасности** выполните следующие действия:

   a. В блоке **Проверка архивов и составных файлов** укажите значения следующих параметров:
      - **Проверять архивы**

        Включение / выключение проверки архивов.

        По умолчанию флажок снят.
      - **Удалять архивы, если лечение не удалось**

        Включение / выключение функции удаления архивов, лечение которых невозможно.

        Если флажок установлен, Kaspersky Security удаляет архивы, которые не удалось вылечить.

        Если флажок снят, программа не удаляет невылеченные архивы. Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию о том, что зараженный файл не удален.

        Флажок доступен для изменения, если установлен флажок **Проверять архивы**.

        По умолчанию флажок снят.
      - **Проверять самораспаковывающиеся архивы**

        Включение / выключение проверки самораспаковывающихся архивов.

        По умолчанию для профилей защиты флажок снят, для задач проверки флажок установлен.
      - **Проверять вложенные OLE-объекты**

        Включение / выключение проверки объектов, вложенных в файл.

По умолчанию флажок установлен.

- **Не распаковывать составные файлы большого размера**

  Если флажок установлен, Kaspersky Security не проверяет составные файлы, размер которых превышает значение поля **Максимальный размер проверяемого составного файла N МБ**.

  Если флажок снят, Kaspersky Security проверяет составные файлы любого размера.

  Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

  По умолчанию флажок установлен.

- **Максимальный размер проверяемого составного файла N МБ**

  Максимальный размер составных файлов, подлежащих проверке (в мегабайтах). Kaspersky Security не распаковывает и не проверяет те объекты, размер которых больше указанного значения.

  Параметр доступен для изменения, если установлен флажок **Не распаковывать составные файлы большого размера**.

  Вы можете указать в этом поле значение от 1 до 999999. По умолчанию задано значение 8 МБ.

b. В блоке **Производительность** укажите значения следующих параметров:

- **Ограничивать время проверки файлов**

  Включение / выключение ограничения времени проверки файлов.

  Если флажок установлен, Kaspersky Security прекращает проверку файла, если время проверки достигает значения, заданного в поле **Проверять файлы не дольше N секунд(ы)**, и пропускает этот файл.

  Если флажок снят, Kaspersky Security не ограничивает время проверки файлов.

  По умолчанию для профилей защиты флажок установлен, для задач проверки флажок снят.

- **Проверять файлы не дольше N секунд(ы)**

  Максимальная длительность проверки файла (в секундах). Kaspersky Security прекращает проверку файла, если она длится больше заданного значения времени.

  Параметр доступен для изменения, если установлен флажок **Ограничивать время проверки файлов**.

  Вы можете указать в этом поле значение от 1 до 3600. По умолчанию задано значение 60 секунд.

c. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка** и укажите в открывшемся окне **Объекты для обнаружения** значения следующих параметров:

- **Вредоносные утилиты**

  Включение / выключение защиты от вредоносных утилит.

  Вредоносные утилиты не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на виртуальной машине. Злоумышленники используют функции вредоносных утилит для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы или других вредоносных действий.

Если флажок установлен, защита от вредоносных утилит включена.

Если флажок снят, защита от вредоносных утилит выключена.

По умолчанию флажок установлен.

- **Программы автодозвона**

  Включение / выключение защиты от программ автодозвона.

  Если флажок установлен, защита от программ автодозвона включена.

  Если флажок снят, защита от программ автодозвона выключена.

  По умолчанию флажок установлен.

- **Рекламные программы**

  Включение / выключение защиты от рекламных программ.

  Рекламные программы связаны с показом пользователю рекламной информации, например: отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-сайты. Некоторые из рекламных программ собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов рекламные программы передают эту информацию разработчику с разрешения пользователя.

  Если флажок установлен, защита от рекламных программ включена.

  Если флажок снят, защита от рекламных программ выключена.

  По умолчанию флажок установлен.

- **Другие**

  Включение / выключение защиты от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя.

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ находятся IRC-клиенты, программы для загрузки файлов, программы удаленного администрирования, программы для отслеживания действий пользователя, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet. Однако если злоумышленники получат доступ к таким программам, они могут использовать некоторые их функции для нанесения вреда виртуальной машине или данным пользователя.

  Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя, включена.

  Если флажок снят, защита от таких программ выключена.

  По умолчанию флажок снят.

- **Многократно упакованные файлы**

  Включение / выключение проверки файлов, которые упакованы одним или несколькими упаковщиками три или более раз.

  Если файл упакован одним или несколькими упаковщиками три или более раз, то существует вероятность, что файл содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Если флажок установлен, защита от многократно упакованных файлов включена, и проверка таких файлов разрешена.

Если флажок снят, защита от многократно упакованных файлов выключена.

По умолчанию флажок установлен.

> Kaspersky Security всегда проверяет файлы виртуальных машин на наличие вирусов, червей и троянских программ. Поэтому параметры **Вирусы и черви** и **Троянские программы** в блоке **Вредоносные программы** недоступны для изменения.

d. Нажмите на кнопку **ОК** в окне **Объекты для обнаружения**.

e. Нажмите на кнопку **ОК** в окне **Параметры уровня безопасности**.

Если вы изменили параметры уровня безопасности, программа создаст пользовательский уровень безопасности. Название уровня безопасности в блоке **Уровень безопасности** изменится на **Пользовательский**.

2. В блоке **Проверка включенных виртуальных машин** настройте параметры проверки виртуальных машин, которые включены во время выполнения задачи:

- **Действие при обнаружении угрозы**

  Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов на включенных виртуальных машинах:

  - **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.
  - **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

    Это действие выбрано по умолчанию.

    Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить, только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.
  - **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.
  - **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

- **Проверять оптические диски**

  Включение / выключение проверки оптических дисков.

  Если флажок установлен, Kaspersky Security проверяет файлы на оптических дисках (CD, DVD, Blu-Ray) при выполнении задачи проверки на виртуальных машинах с операционными системами Windows.

  Если флажок снят, Kaspersky Security не проверяет файлы на оптических дисках.

  Если флажок установлен, но для задачи задана область проверки, в которую не

включен путь к оптическому диску, Kaspersky Security не проверяет файлы на оптическом диске.

Kaspersky Security не проверяет файлы на оптических дисках при проверке выключенных виртуальных машин, шаблонов виртуальных машин и виртуальных машин с операционными системами Linux.

По умолчанию флажок снят.

3. В блоке **Проверка выключенных виртуальных машин и шаблонов виртуальных машин** настройте параметры проверки виртуальных машин, которые выключены или приостановлены во время выполнения задачи, а также шаблонов виртуальных машин:

   - **Проверять выключенные виртуальные машины**

     Включение / выключение проверки выключенных виртуальных машин.

     Если флажок установлен, при выполнении задачи проверки Kaspersky Security проверяет файлы на выключенных виртуальных машинах, входящих в область действия задачи, с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS. Файлы на выключенных виртуальных машинах с другими файловыми системами не проверяются.

     Во время проверки выключенную виртуальную машину невозможно включить или выполнить ее миграцию.

     Если флажок снят, Kaspersky Security не проверяет файлы на выключенных виртуальных машинах.

     По умолчанию флажок снят.

   - **Проверять шаблоны виртуальных машин**

     Включение / выключение проверки шаблонов виртуальных машин.

     Если флажок установлен, при выполнении задачи проверки Kaspersky Security проверяет файлы на шаблонах виртуальных машин, входящих в область действия задачи.

     Если флажок снят, Kaspersky Security не проверяет файлы на шаблонах виртуальных машин.

     По умолчанию флажок снят.

     Флажок доступен, если установлен флажок **Проверять выключенные виртуальные машины**.

   - **Действие при обнаружении угрозы**

     Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов на выключенных виртуальных машинах или шаблонах виртуальных машин:

     - **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.
     - **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

       Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить,

только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.

- **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.
- **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

  Это действие выбрано по умолчанию.

Выбор действия доступен, если установлен флажок **Проверять выключенные виртуальные машины**.

4. В блоке **Останавливать проверку** выберите один из следующих вариантов:
   - **По истечении N минут(ы) с момента запуска задачи**

     Максимальное время выполнения задачи проверки (в минутах). По достижении заданного времени выполнение задачи проверки прекращается, даже если проверка не была завершена.

     Этот вариант выбран по умолчанию.

     Вы можете указать в этом поле значение от 1 до 4320. По умолчанию указано значение 120 минут.
   - **После окончания проверки файлов на всех защищенных виртуальных машинах**

     Задача проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах, входящих в область действия задачи.
5. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Настройка области проверки в задаче проверки

Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Если область проверки не настроена, Kaspersky Security проверяет все файлы виртуальных машин.

При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется создать задачу проверки виртуальных машин, папки и файлы которых открыты для сетевого доступа, и включить эти папки и файлы в область проверки задачи.
При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

Вы можете сформировать область проверки задачи во время создания задачи (шаг **Выбор области проверки**) или в свойствах задачи после ее создания (раздел **Область проверки**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить область проверки задачи, выполните следующие действия:*

1. Выберите один из следующих вариантов:
   - **Проверять все папки и файлы, кроме указанных**.
   - **Проверять только указанные папки и файлы**.
2. Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, вы можете сформировать список объектов, которые требуется исключить из области проверки, с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

   Вы можете исключать из области проверки объекты следующих типов:

   - Папки. Из области проверки исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение к вложенным папкам.
   - Файлы по маске. Из области проверки исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

     При указании маски файла вы можете использовать символы `*` и `?`.

     Kaspersky Security не учитывает регистр символов в путях к файлам и папкам, именах и масках файлов, которые требуется исключить из области проверки.

   Вы можете сохранить настроенный список исключений в файл с помощью кнопки **Экспорт** и загрузить ранее сохраненный список исключений из файла с помощью кнопки **Импорт**. Для импорта и экспорта списка исключений вы можете использовать файл в формате XML. Импортировать список исключений вы также можете из файла в формате DAT. С помощью файла в формате DAT вы можете импортировать список исключений, сформированный в других программах "Лаборатории Касперского".

   В комплект поставки программы входит файл microsoft_file_exclusions.xml, который содержит список исключений, рекомендуемых корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Файл microsoft_file_exclusions.xml расположен в папке установки плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Вы можете импортировать этот файл в исключения задачи проверки. После выполнения импорта Kaspersky Security не проверяет объекты, рекомендуемые корпорацией Microsoft, во время выполнения задачи проверки. Вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы**.

Если вы используете в списке исключений переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows из области проверки исключаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, из области проверки исключаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

3. Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, в блоке **Расширения файлов** вы можете указать расширения файлов, которые нужно включить в область проверки или исключить из области проверки.

   Для этого выберите один из следующих вариантов:

   - **Проверять все, кроме файлов со следующими расширениями**. В поле ввода укажите список расширений файлов, которые не надо проверять во время выполнения задачи проверки. Kaspersky Security не учитывает регистр символов в расширениях файлов, которые требуется исключить из области проверки.
   - **Проверять только файлы со следующими расширениями**. В поле ввода укажите список расширений файлов, которые надо проверять во время выполнения задачи проверки. При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в расширениях файлов, которые требуется включить в область проверки. При проверке виртуальных машин с операционными системами Windows регистр символов в расширениях файлов не учитывается.

     Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

     Если вы выбрали в раскрывающемся списке вариант **Проверять только файлы со следующими расширениями**, но не указали расширения файлов, которые надо проверять, Kaspersky Security проверяет все файлы.

   Исключенные из проверки папки имеют более высокий приоритет, чем расширения файлов, включенные в область проверки. Если файл находится в папке, исключенной из проверки, то программа не проверяет его, несмотря на то, что расширение файла включено в область проверки.

4. Если вы выбрали вариант **Проверять только указанные папки и файлы**, с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список папок и файлов на виртуальной машине, которые нужно проверять во время выполнения задачи проверки.

   При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в путях к файлам и директориям, включаемым в область проверки. При проверке виртуальных машин с операционными системами Windows регистр символов в путях к файлам и папкам не учитывается.

Если в списке объектов, которые нужно проверять, вы используете переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows в область проверки включаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, в область проверки включаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

5. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Настройка области действия задачи выборочной проверки

Вы можете настроить область действия задачи выборочной проверки во время создания задачи (шаг **Настройка области действия задачи**) или в свойствах задачи после ее создания (раздел **Область действия задачи**).

Задача выборочной проверки, созданная с помощью основного плагина управления

Для задачи выборочной проверки, созданной с помощью основного плагина управления Kaspersky Security, вы можете настроить область действия задачи одним из следующих способов:

- Указать виртуальные машины и / или шаблоны виртуальных машин, файлы которых вы хотите проверить.
- Указать одну или несколько групп безопасности NSX (NSX Security Group), в которые включены виртуальные машины. Kaspersky Security проверит файлы всех виртуальных машин, которые включены в указанные группы безопасности NSX.

► *Чтобы настроить область действия задачи выборочной проверки, созданной с помощью основного плагина управления, выполните следующие действия:*

1. Если вы хотите включить в область действия задачи виртуальные машины и / или шаблоны виртуальных машин, в раскрывающемся списке в верхней части окна выберите вариант **Объекты виртуальной инфраструктуры** (этот вариант выбран по умолчанию). В окне отобразится виртуальная инфраструктура VMware под управлением одного сервера VMware vCenter Server в виде дерева объектов: VMware vCenter Server, объекты Datacenter, кластеры VMware, ресурсные пулы, объекты vApp и виртуальные машины.

   Установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

   Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

2. Если вы хотите включить в область действия задачи все виртуальные машины, входящие в одну или несколько групп безопасности NSX, в раскрывающемся списке в верхней части окна выберите вариант **Группы безопасности NSX**.

   Установите флажки для групп безопасности NSX, виртуальные машины которых вы хотите проверить во время выполнения создаваемой задачи.

   > Если областью действия задачи является одна или несколько групп безопасности NSX, во время выполнения этой задачи Kaspersky Security не проверяет шаблоны виртуальных машин, даже если в параметрах проверки установлен флажок **Проверять шаблоны виртуальных машин**.

3. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Задача выборочной проверки, созданная с помощью плагина управления для клиентов

Для задачи выборочной проверки, созданной с помощью плагина управления Kaspersky Security для клиентов, недоступно формирование области действия задачи с помощью групп безопасности NSX. Вы можете включать в область действия задач отдельные виртуальные машины или их объединения.

► *Чтобы настроить область действия задачи выборочной проверки, созданной с помощью плагина управления для клиентов, выполните следующие действия:*

1. Установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

   > Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

2. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Настройка расписания запуска задач проверки

Вы можете настроить расписание запуска задач проверки во время создания задачи (шаг **Настройка расписания запуска задачи**) или в свойствах задачи после ее создания (раздел **Расписание**).

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Определите значения следующих параметров:

   - **Запуск по расписанию**. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.
   - **Запускать пропущенные задачи**. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов **Вручную** и **Один раз** задача запускается сразу после появления SVM в сети.

Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов **Вручную** и **Один раз** – только на видимых в сети SVM.

- **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:
  - 0–200 SVM – запуск задачи не распределяется;
  - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
  - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
  - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
  - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
  - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
  - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
  - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
  - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

  Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию флажок установлен.
- **Использовать случайную задержку запуска задачи в интервале (мин)**. Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

  Распределенный запуск задачи помогает избежать одновременного обращения большого количества SVM к Серверу администрирования Kaspersky Security Center.

2. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

kaspersky

Резервное хранилище

Резервное хранилище – это специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

Резервная копия файла – копия файла с виртуальной машины, которая создается при лечении или удалении этого файла. Резервные копии файлов хранятся в резервном хранилище в специальном формате и не представляют опасности.

Когда программа Kaspersky Security обнаруживает зараженный файл на виртуальной машине, она закрывает пользователю виртуальной машины доступ к этому файлу, а затем помещает его копию в резервное хранилище. Далее программа выполняет над файлом то действие, которое указано в профиле защиты этой виртуальной машины, например лечит или удаляет файл.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал информацию, которая в результате лечения стала полностью или частично недоступна, вы можете сохранить файл из резервной копии на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Резервное хранилище располагается на SVM с установленным компонентом Защита от файловых угроз. По умолчанию на каждой SVM включено использование резервного хранилища.

Объем резервного хранилища на SVM составляет 1 ГБ. Если суммарный объем резервных копий файлов в резервном хранилище превышает это значение, программа Kaspersky Security удаляет резервные копии файлов, помещенные туда ранее остальных, чтобы сохранить размер резервного хранилища равным 1 ГБ.

По умолчанию максимальный срок хранения резервных копий файлов в резервном хранилище составляет 30 дней. По истечении этого времени Kaspersky Security автоматически удаляет резервные копии файлов из резервного хранилища.

Вы можете изменить максимальный срок хранения резервных копий файлов. Параметры резервного хранилища настраиваются в параметрах политики для всех SVM в составе одного кластера KSC (см. раздел "Настройка параметров резервного хранилища" на стр. 122).

Вы можете работать с резервными копиями файлов, которые находятся в резервных хранилищах на SVM, в Консоли администрирования Kaspersky Security Center. В Консоли администрирования Kaspersky Security Center представлен общий список резервных копий файлов, помещенных программой Kaspersky Security в резервное хранилище на каждой SVM с установленным компонентом Защита от файловых угроз.

В этом разделе

kaspersky

Настройка параметров резервного хранилища

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры резервного хранилища на SVM, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики выберите раздел **Резервное хранилище**.
3. В правой части окна настройте следующие параметры:
   - Если вы хотите, чтобы программа Kaspersky Security не помещала в резервное хранилище резервную копию файла перед его лечением или удалением, снимите флажок **Помещать файлы в резервное хранилище**. По умолчанию флажок установлен.

     Если вы использовали резервное хранилище, а потом сняли этот флажок, в резервном хранилище останутся резервные копии файлов, помещенные туда ранее. Эти резервные копии файлов будут удалены по мере действия параметра **Хранить файлы не более N дней**.
   - Если требуется, в поле **Хранить файлы не более N дней** измените срок хранения резервных копий файлов в резервном хранилище. По истечении этого времени Kaspersky Security автоматически удаляет резервные копии файлов из резервного хранилища. По умолчанию задано значение 30 дней.

     Если вы уменьшили срок хранения резервных копий файлов, Kaspersky Security в течение суток удалит из резервного хранилища те копии, которые находятся там дольше нового срока хранения.
4. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

kaspersky

Работа с резервными копиями файлов

Вы можете выполнять следующие действия с резервными копиями файлов:

- просматривать список резервных копий файлов;
- сохранять файлы из резервных копий на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center;
- удалять резервные копии файлов из резервного хранилища.

► *Чтобы открыть список резервных копий файлов,*

в Консоли администрирования Kaspersky Security Center в папке **Дополнительно** → **Хранилища** выберите папку **Резервное хранилище**.

В рабочей области отобразится список резервных копий файлов, помещенных в резервные хранилища на всех SVM.

Список резервных копий файлов представлен в виде таблицы. Каждая строка таблицы содержит событие, произошедшее с зараженным файлом, и информацию об обнаруженном в файле объекте.

В графах таблицы отображается следующая информация:

- **Устройство** – имя и путь к виртуальной машине, на которой обнаружен файл.
- **Имя** – имя файла.
- **Статус** – статус, который программа Kaspersky Security присвоила обнаруженному файлу после обработки: *Удален*, *Вылечен*.
- **Выполняемое действие** – действие, которое на текущий момент выполняет программа с этой резервной копией файла в резервном хранилище. Например, если вы дали команду удалить резервную копию файла, то в этой графе отображается *Удаляется*. Если программа не выполняет действий над этой резервной копией файла, то это поле пусто.
- **Дата помещения** – дата и время помещения резервной копии файла в резервное хранилище.
- **Объект** – название объекта, обнаруженного в файле. Если в файле обнаружено несколько объектов, то в списке резервных копий файлов каждый обнаруженный объект отображается на отдельной строке.
- **Размер** – размер файла в байтах.
- **Папка восстановления** – полный путь к исходному файлу на виртуальной машине.
- **Описание** – имя виртуальной машины и полный путь на ней к исходному файлу, резервная копия которого помещена в резервное хранилище.

► *Чтобы сохранить файл из резервного хранилища на диск, выполните следующие действия:*

1. В списке резервных копий файлов выберите файл, который вы хотите сохранить на диск.
2. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Сохранить на диск**.
   - Сохраните файл по ссылке **Сохранить на диск**. Ссылка находится в блоке работы с выбранным файлом, справа от списка резервных копий файлов.

Откроется окно для выбора папки на жестком диске компьютера, в которую требуется сохранить выбранный файл.

3. Выберите папку на жестком диске компьютера, в которую вы хотите сохранить файл.
4. Нажмите на кнопку **ОК**.

Kaspersky Security сохранит указанный вами файл на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Файлы сохраняются на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center, в незашифрованном виде.

► *Чтобы удалить резервные копии файлов, выполните следующие действия:*

1. В списке резервных копий файлов выберите файлы, которые вы хотите удалить. Используйте клавиши **CTRL** и **SHIFT**, чтобы выбрать несколько файлов.
2. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.
   - Удалите файлы по ссылке **Удалить объекты**. Ссылка находится в блоке работы с выбранными файлами, справа от списка резервных копий файлов.

Kaspersky Security удалит резервные копии файлов из резервных хранилищ на SVM. По ссылке **Обновить** вы можете обновить список резервных копий файлов, чтобы увидеть изменения в списке.

Обновление списка резервных копий файлов занимает некоторое время, дождитесь его завершения.

kaspersky

Обновление баз программы

Базы программы содержат описания угроз компьютерной безопасности, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Обновление баз программы обеспечивает актуальность защиты виртуальных машин. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах программы. Чтобы программа Kaspersky Security своевременно обнаруживала угрозы, вам нужно регулярно обновлять базы программы.

Для обновления баз программы требуется действующая лицензия на использование программы.

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы для программ "Лаборатории Касперского". Источником обновлений для Kaspersky Security является хранилище Сервера администрирования Kaspersky Security Center.

Чтобы успешно загрузить пакет обновлений из хранилища Сервера администрирования, SVM должна иметь доступ к Серверу администрирования Kaspersky Security Center.

Если базы программы давно не обновлялись, то пакет обновлений может иметь значительный размер (до нескольких десятков мегабайт). Загрузка такого пакета обновлений может создать дополнительную нагрузку на сеть.

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления баз программы на SVM (см. раздел «Настройка автоматического обновления баз программы» на стр. 125). Для этого используются следующие задачи:

- **Задача загрузки обновлений в хранилище**. Задача позволяет загружать пакет обновлений из источника обновлений в хранилище Сервера администрирования Kaspersky Security Center.
- **Задача обновления баз программы**. Задача позволяет распространять и устанавливать обновления баз программы на SVM сразу после загрузки пакета обновлений в хранилище Сервера администрирования.

В этом разделе

Настройка автоматического обновления баз программы

► *Чтобы настроить автоматическое обновление баз программы, выполните следующие действия:*

1. Убедитесь, что в Kaspersky Security Center создана задача загрузки обновлений в хранилище.

Задача загрузки обновлений в хранилище создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Если задача загрузки обновлений в хранилище была удалена из списка задач Сервера администрирования, вы можете создать новую задачу. См. подробнее в документации Kaspersky Security Center.

2. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы.

   Задача обновления баз программы может быть создана автоматически (см. раздел "Политики и задачи по умолчанию" на стр. 45) после установки основного плагина управления Kaspersky Security. Вы можете использовать эту задачу для обновления баз программы.

3. Если задача отсутствует, создайте ее следующим образом.

   a. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:

      - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите создать задачу для всех SVM. В рабочей области выберите закладку **Задачи**.
      - В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для SVM которого вы хотите создать задачу. В рабочей области выберите закладку **Задачи**.
      - Выберите папку **Задачи** дерева консоли, если вы хотите создать задачу для одной или нескольких SVM.

   b. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.

   c. На первом шаге мастера выберите тип задачи: **Kaspersky Security для виртуальных сред 6.0 Защита без агента → Обновление**. Перейдите к следующему шагу мастера создания задачи.

   d. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM, для которых вы создаете задачу. Вы можете выбрать SVM из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать список SVM из файла или указать ранее настроенную выборку SVM (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

      - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия SVM.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

      Перейдите к следующему шагу мастера создания задачи.

   e. В поле **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**.

      Выбор другого варианта запуска задачи приводит к выходу программы из сертифицированного состояния.

      Настройте остальные параметры расписания запуска задачи. Подробнее о параметрах расписания запуска задач см. в документации Kaspersky Security Center. Перейдите к следующему шагу мастера создания задачи.

f. В поле **Имя** введите имя задачи обновления баз программы. Перейдите к следующему шагу мастера создания задачи.

g. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**. Завершите работу мастера создания задачи. Созданная задача обновления баз программы отобразится в списке задач.

Задача будет запускаться каждый раз при загрузке пакета обновлений в хранилище Сервера администрирования, распространять и устанавливать обновления баз программы на SVM. Вы можете посмотреть результаты ее выполнения и при необходимости запустить задачу вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

При обновлении баз программы Kaspersky Security проверяет их целостность. Если проверка закончилась неудачно, задача обновления баз программы завершается с ошибкой и Kaspersky Security продолжает использовать предыдущий набор баз программы.

Откат последнего обновления баз программы

После первого обновления баз программы доступен откат к предыдущему набору баз.

Каждый раз, когда на SVM запускается обновление, Kaspersky Security создает резервную копию используемых баз программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущего набора баз программы при необходимости. Возможность отката последнего обновления используется, например, в том случае, если новая версия баз программы содержит некорректную сигнатуру, из-за которой Kaspersky Security блокирует безопасную программу.

► *Чтобы откатить последнее обновление баз программы, выполните следующие действия:*

1. Создайте задачу отката обновления следующим образом:

   a. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:

      - Выберите папку **Управляемые устройства** дерева консоли, если вы хотите откатить обновление баз программы на всех SVM. В рабочей области выберите закладку **Задачи**.
      - В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для SVM которого вы хотите откатить обновление баз программы. В рабочей области выберите закладку **Задачи**.
      - Выберите папку **Задачи** дерева консоли, если вы хотите откатить обновление баз программы на одной или нескольких SVM.

   b. Нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.

   c. На первом шаге мастера выберите тип задачи: **Kaspersky Security для виртуальных сред 6.0 Защита без агента → Откат обновления**. Перейдите к следующему шагу мастера создания задачи.

   d. Если вы запустили мастер создания задачи из папки **Задачи**, укажите способ выбора SVM, на которых должна выполняться задача. Вы можете выбрать SVM из списка виртуальных машин, обнаруженных Сервером администрирования, задать адреса SVM вручную, импортировать

список SVM из файла или указать ранее настроенную выборку SVM (см. подробнее в документации Kaspersky Security Center). В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

- В списке обнаруженных виртуальных машин укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия SVM.
- Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса SVM вручную.
- Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
- Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.

Перейдите к следующему шагу мастера создания задачи.

e. В поле **Запуск по расписанию** выберите **Вручную**. Настройте остальные параметры расписания запуска задачи. Подробнее о параметрах расписания запуска задач см. в документации Kaspersky Security Center. Перейдите к следующему шагу мастера создания задачи.

f. В поле **Имя** введите имя задачи отката обновления. Перейдите к следующему шагу мастера создания задачи.

g. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**. Завершите работу мастера создания задачи. Созданная задача отката обновления отобразится в списке задач.

2. Если вы не настроили запуск задачи после завершения работы мастера, запустите задачу отката обновления вручную (см. раздел "О задачах Kaspersky Security" на стр. 24).

kaspersky

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальных машин, Kaspersky Security может использовать данные, полученные от пользователей программ "Лаборатории Касперского" во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Если вы участвуете в Kaspersky Security Network, программа Kaspersky Security получает от служб KSN сведения о категории и репутации проверяемых файлов.

В зависимости от расположения инфраструктуры KSN различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского". Если вы используете Глобальный KSN, Kaspersky Security автоматически отправляет в "Лабораторию Касперского" информацию об использовании KSN, а также может отправлять другую информацию в зависимости от выбранного вами режима использования KSN (*стандартный KSN* или *расширенный KSN*). Режим KSN влияет на объем данных, которые передаются в "Лабораторию Касперского" при использовании KSN.
- Локальный KSN – инфраструктура расположена внутри корпоративной сети организации или на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера.

Информация о том, какой тип KSN использует программа Kaspersky Security, отображается в свойствах политики.

Использование Глобального KSN независимо от выбранного режима использования KSN (стандартный KSN или расширенный KSN) приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Для использования Локального KSN требуется включить и настроить использование Локального KSN в Kaspersky Security Center. Настройка Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

Настройка использования KSN в работе программы Kaspersky Security выполняется в свойствах политики.

Участие в Kaspersky Security Network является добровольным. Решение об участии в Kaspersky Security Network принимается при создании политики Kaspersky Security, можно изменить его в любой момент.

► *Чтобы настроить использование Kaspersky Security Network, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).

b. В рабочей области выберите закладку **Политики**.

c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.

2. В окне свойств политики выберите раздел **Параметры KSN**.
3. Если вы хотите использовать Локальный KSN в работе программы, установите флажок **Использовать Локальный KSN**.
4. Если вы хотите выключить использование Локального KSN, снимите флажок **Использовать Локальный KSN**.
5. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

kaspersky

SNMP-мониторинг состояния SVM

Вы можете получать информацию о состоянии SVM, развернутых в виртуальной инфраструктуре, с помощью любой системы сетевого управления, использующей протокол SNMP. На SVM установлен агент SNMP, который может передавать информацию о состоянии SVM системе сетевого управления вашей организации.

Агент SNMP может передавать следующие сведения о состоянии SVM с компонентом Защита от файловых угроз:

- Информацию об использовании оперативной памяти процессом ksvmain в процентах (относительно максимального значения, при достижении которого программа перезапускается).
- Количество защищенных виртуальных машин с операционными системами для рабочих станций и количество защищенных виртуальных машин с операционными системами для серверов.

  При подсчете количества защищенных виртуальных машин учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены.

- Информацию о том, выполняются ли на SVM в текущий момент задачи проверки виртуальных машин.
- Если задачи проверки выполняются, информацию о количестве виртуальных машин, которые ожидают проверки в текущий момент времени, и о количестве одновременно проверяемых виртуальных машин.
- Информацию о состоянии служб компонента Защита от файловых угроз на SVM: *On* (службы запущены) или *Off* (службы не запущены).

Эти данные специфичны для программы, информация о них содержится в MIB-файлах KSV-MIB.txt и KSVNS-MIB.txt, которые поставляются вместе с программой. Вы можете использовать эти файлы для получения дополнительной информации от SVM. Вы можете также использовать другие MIB-файлы для получения необходимой информации от SVM.

Включение и выключение SNMP-мониторинга выполняется в параметрах политики. Если в активной политике, которая определяет параметры работы SVM, SNMP-мониторинг включен, агент SNMP, установленный на SVM, передает информацию о состоянии SVM системе SNMP-мониторинга вашей организации.

Если политика, в которой включен SNMP-мониторинг, не активна, информация о состоянии SVM не передается.

► *Чтобы настроить параметры SNMP-мониторинга, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики**.

c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.

2. В окне свойств политики выберите раздел **Параметры SNMP-мониторинга**.
3. Выполните одно из следующих действий:

   - Если вы хотите получать информацию о состоянии SVM, установите флажок **Включить SNMP-мониторинг состояния SVM**.

     Вы можете ограничить список IP-адресов, на которые агент SNMP передает информацию о состоянии SVM, чтобы предотвратить несанкционированный доступ к службе SNMP. Чтобы сформировать список IP-адресов, на которые передается информация о состоянии SVM, выполните следующие действия:

     a. Установите флажок **Передавать информацию только на указанные IP-адреса**.

     b. Нажмите на кнопку **Добавить** или на клавишу **INSERT** и введите в строке списка IP-адрес в формате IPv4 или IP-подсеть в следующем формате: <IP-адрес в формате IPv4>/<количество единичных разрядов в маске подсети>.

   - Если вы хотите выключить мониторинг состояния SVM, снимите флажок **Включить SNMP-мониторинг состояния SVM**

4. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

kaspersky

События

SVM отправляют на Сервер администрирования Kaspersky Security Center служебные сообщения с информацией о работе Kaspersky Security – *события*. Информация о событиях сохраняется в базе данных Сервера администрирования.

Выделяют следующие уровни важности событий:

- **Критическое событие**. Событие критической важности, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке. Может указывать на проблемы в работе Kaspersky Security или на уязвимости в защите виртуальных машин.
- **Отказ функционирования**. Событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- **Предупреждение**. Событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky Security и может указывать на возможную проблему в будущем.
- **Информационное сообщение**. Событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

Список всех событий в работе Сервера администрирования, управляемых устройств и программ сохраняется в журнале событий Kaspersky Security Center и отображается в Консоли администрирования Kaspersky Security Center (см. раздел "Просмотр событий" на стр. 133).

Уведомление – это сообщение с информацией о событии, которое произошло на SVM. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе программы. Kaspersky Security Center позволяет выбирать способ уведомления о событиях и настраивать параметры уведомлений о событиях в свойствах политики (см. раздел "Настройка параметров уведомлений о событиях" на стр. 134).

Подробную информацию о событиях и уведомлениях см. в документации Kaspersky Security Center.

В событиях Kaspersky Security Center в качестве имени виртуальной машины может отображаться имя виртуальной машины и путь к ней в виртуальной инфраструктуре.

В этом разделе

Просмотр событий

► *Чтобы открыть список всех событий в работе Сервера администрирования Kaspersky Security Center, управляемых устройств и программ,*

в Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования** и перейдите на закладку **События** в рабочей области узла.

В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **События выборки**. События в списке не обновляются автоматически. Чтобы просмотреть самые последние события, обновите список по ссылке **Обновить**.

Вы можете выполнять следующие действия при просмотре событий:

- Выбирать выборку, события из которой должны отображаться в списке. Раскрывающийся список **События выборки** содержит предопределенные выборки (созданные по умолчанию), а также пользовательские выборки. Если пользователь не создавал собственные выборки, пользовательских выборок нет в списке.
- Добавлять или удалять графы из списка событий.
- Искать события в списке по ключевым словам.
- Просматривать подробную информацию о событии, выбранном в списке. Поле с подробной информацией о событии находится справа от списка событий.
- Создавать и настраивать выборки событий.
- Экспортировать и импортировать события выборки.
- Настраивать уведомления о событиях и экспорт событий в SIEM-систему.

Подробную информацию о работе с событиями см. в документации Kaspersky Security Center.

Настройка параметров уведомлений о событиях

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры уведомлений о событиях, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:
   a. В дереве консоли выберите папку или группу администрирования, в которой создана политика (см. раздел "Особенности использования политик Kaspersky Security" на стр. 22).
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики выберите раздел **Настройка событий**.
3. Выберите закладку с названием уровня важности событий, о которых вы хотите получать уведомления:

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

4. Выберите типы событий, о которых вы хотите получать уведомления:
   - Используйте клавиши **SHIFT** и **CTRL**, если вы хотите выбрать несколько типов событий.
   - Нажмите на кнопку **Выбрать все**, если вы хотите выбрать все типы событий.
5. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства <N событий>**, где N – количество выбранных типов событий.
6. В блоке **Регистрация событий** установите флажок **На Сервере администрирования в течение (сут)**. Kaspersky Security будет отправлять на Сервер администрирования Kaspersky Security Center события выбранных вами типов.

   В поле ввода укажите количество дней, в течение которых события должны храниться на Сервере администрирования. Kaspersky Security Center удаляет события по истечении заданного времени.
7. В блоке **Уведомления о событиях** выберите способ уведомления:
   - **Уведомлять по электронной почте**.
   - **Уведомлять по SMS**.
   - **Уведомлять запуском исполняемого файла или скрипта**.
   - **Уведомлять по SNMP**.
8. Нажмите на кнопку **ОК** в окне **Свойства <N событий>**.
9. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

kaspersky

Инструкция по работе с программой для администратора организации-клиента

Этот раздел адресован администратору виртуальной инфраструктуры, которая принадлежит организации-клиенту и находится под защитой программы Kaspersky Security, установленной в инфраструктуре организации-провайдера антивирусной защиты.

Этот раздел содержит сведения, необходимые администратору клиента для управления защитой своей виртуальной инфраструктуры.

Для работы с программой Kaspersky Security требуется опыт работы с виртуальной инфраструктурой на платформе VMware vSphere и системой удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center.

В этом разделе

Об управлении программой

Управление Kaspersky Security осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center.

Интерфейс для управления программой Kaspersky Security через Kaspersky Security Center обеспечивает *плагин управления Kaspersky Security для клиентов*. Плагин управления должен быть установлен на том компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

Управление работой программы Kaspersky Security осуществляется с помощью политик и задач.

Политика – это набор параметров, с которыми SVM защищают виртуальные машины, входящие в состав защищаемой инфраструктуры. Каждая политика содержит один или несколько *профилей защиты*. Профили защиты позволяют настроить параметры файловой защиты виртуальных машин (см. раздел "О политиках и профилях защиты" на стр. 137).

Задачи запускаются на SVM и позволяют выполнять проверку виртуальных машин (см. раздел "О задачах" на стр. 138).

Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время антивирусной защиты и проверки виртуальных машин, а также о событиях, произошедших во время защиты от вторжений и проверки веб-адресов. Вы можете получать уведомления о событиях и просматривать их в Kaspersky Security Center (см. раздел "Получение информации о состоянии защиты" на стр. 169).

kaspersky

Подробную информацию о работе с событиями, политиками и задачами см. в документации Kaspersky Security Center.

В этом разделе

О политиках и профилях защиты

Политика позволяет настраивать параметры файловой защиты виртуальных машин с помощью профилей защиты, а также параметры использования Kaspersky Security Network.

Термин "профиль защиты", используемый в этом документе, не следует путать с термином "профиль защиты" в нотации ГОСТ Р ИСО/МЭК 15408.

В политиках Kaspersky Security предусмотрены следующие профили защиты:

- *Основной профиль защиты* автоматически формируется во время создания политики. Основной профиль защиты недоступен для удаления, однако вы можете изменять значения параметров основного профиля защиты.
- *Дополнительные профили защиты* вы можете создать после создания политики. Благодаря дополнительным профилям защиты вы можете гибко настраивать разные параметры защиты для разных виртуальных машин в составе защищаемой инфраструктуры. Политика может содержать несколько дополнительных профилей защиты.

В профилях защиты вы можете настраивать следующие параметры:

- Уровень безопасности. Вы можете выбрать один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**) или настроить уровень безопасности самостоятельно (**Пользовательский**). Уровень безопасности определяет следующие параметры проверки:
  - проверка архивов, самораспаковывающихся архивов, вложенных OLE-объектов, составных файлов;
  - ограничение проверки файлов по времени;
  - список объектов для обнаружения.
- Действие, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы.
- Область защиты (проверка сетевых дисков во время защиты виртуальных машин).
- Исключения из защиты (по имени, расширению или пути к файлу, по маске файла или по пути к папке, файлы которой не надо проверять).

Профиль защиты может быть назначен отдельному объекту виртуальной инфраструктуры VMware или корневому элементу защищаемой инфраструктуры, в роли которого выступает условный объект "Организация vCloud Director". Профиль защиты, назначенный корневому элементу защищаемой инфраструктуры, по умолчанию наследуется всеми дочерними элементами защищаемой инфраструктуры (виртуальными машинами и их объединениями).

Профили защиты наследуются также согласно иерархии объектов виртуальной инфраструктуры VMware: профиль защиты, назначенный объекту виртуальной инфраструктуры, наследуется всеми его дочерними объектами, в том числе и виртуальными машинами, если дочернему объекту / виртуальной машине не назначен собственный профиль защиты (см. раздел "Назначение профиля защиты виртуальным машинам" на стр. 153) или если дочерний объект / виртуальная машина не исключены из защиты (см. раздел "Выключение защиты виртуальных машин от файловых угроз" на стр. 154). Таким образом, вы можете назначить виртуальной машине собственный профиль защиты или использовать для нее профиль защиты, унаследованный от родительского объекта.

Одному объекту виртуальной инфраструктуры может быть назначен только один профиль защиты. Kaspersky Security защищает виртуальные машины с теми параметрами, которые указаны в назначенном этим виртуальным машинам профиле защиты.

Объекты виртуальной инфраструктуры, которым не назначен профиль защиты, исключаются из защиты.

Если вы исключаете объект виртуальной инфраструктуры из защиты, то все дочерние объекты, у которых профиль защиты унаследован от родительского объекта, тоже исключаются из защиты. Вы можете исключить из защиты все дочерние объекты, которым назначен собственный профиль защиты, или оставить их под защитой программы.

Наследование профилей защиты позволяет назначать одинаковые параметры защиты нескольким виртуальным машинам одновременно. Например, вы можете назначить одинаковые профили защиты всем виртуальным машинам в составе виртуального Datacenter.

Политики создаются с помощью мастера, который запускается по кнопке **Новая политика**, расположенной в рабочей области папки **Управляемые устройства** на закладке **Политики** (см. раздел "**Создание политики**" на стр. 141).

Вы можете создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

Вы можете изменять параметры политики после ее создания в окне свойств политики.

► *Чтобы открыть окно свойств политики, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Политики**.
3. В списке политик выберите политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши по политике или выбрав в контекстном меню пункт **Свойства**.

Подробнее о работе с политиками см. в документации Kaspersky Security Center.

О задачах

Для Kaspersky Security предусмотрены следующие задачи:

- Задача полной проверки виртуальных машин. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин в вашей виртуальной инфраструктуре.
- Задача выборочной проверки виртуальных машин. Задача позволяет выполнять антивирусную проверку файлов тех виртуальных машин, которые вы указали в параметрах задачи. Вы можете указывать отдельные виртуальные машины или объекты виртуальной инфраструктуры VMware более высокого уровня иерархии.

Задачи создаются с помощью мастера, который запускается по кнопке **Новая задача**, расположенной в рабочей области папки **Управляемые устройства** на закладке **Задачи**.

Вы можете изменять параметры задачи после ее создания в окне свойств задачи.

► *Чтобы открыть окно свойств задачи, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Задачи**.
3. В списке задач выберите задачу и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши по задаче или выбрав в контекстном меню пункт **Свойства**.

Вне зависимости от выбранного режима запуска задачи вы можете запускать и останавливать задачи в любой момент.

► *Чтобы запустить или остановить задачу, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Задачи**.
3. В списке задач выберите задачу, которую вы хотите запустить или остановить.
4. Нажмите на кнопку **Запустить** или на кнопку **Остановить**. Кнопки расположены справа от списка задач.

Информацию о ходе и результатах выполнения задач вы можете посмотреть в Консоли администрирования Kaspersky Security Center одним из следующих способов:

- В окне **Результаты выполнения задачи**. Окно открывается по ссылке **Просмотреть результаты**, расположенной справа от списка задач, который отображается на закладке **Задачи** в рабочей области папки **Управляемые устройства**.
- В списке событий, который отображается на закладке **События** в рабочей области узла **Сервер администрирования**.

Вы также можете выполнять следующие действия с задачами:

- копировать задачи из одной папки или группы администрирования в другую;
- экспортировать задачи в файл и импортировать задачи из файла;
- конвертировать задачи предыдущей версии программы;
- удалять задачи.

Подробнее об управлении задачами см. в документации Kaspersky Security Center.

kaspersky

Развертывание защиты виртуальной инфраструктуры организации-клиента

Развертывание защиты виртуальной инфраструктуры организации-клиента состоит из следующих этапов:

1. Установка и настройка всех компонентов программы Kaspersky Security в виртуальной инфраструктуре организации-провайдера антивирусной защиты. Все действия на этом этапе выполняет администратор провайдера.
2. Установка Консоли администрирования Kaspersky Security Center на рабочем месте администратора организации-клиента. С помощью Консоли администрирования Kaspersky Security Center вы можете управлять параметрами файловой защиты и параметрами проверки ваших виртуальных машин, а также получать информацию о событиях, которые происходят во время защиты вашей виртуальной инфраструктуры. Подробнее об установке Консоли администрирования см. в документации Kaspersky Security Center.
3. Установка плагина управления Kaspersky Security для клиентов на рабочем месте администратора организации-клиента (см. раздел "Установка плагина Kaspersky Security для клиентов" на стр. 140).
4. Подключение к виртуальному Серверу администрирования Kaspersky Security Center. Вам нужно запустить Консоль администрирования Kaspersky Security Center и указать параметры подключения к виртуальному Серверу администрирования, предоставленные провайдером: адрес, имя пользователя и пароль учетной записи.
5. Настройка параметров защиты виртуальных машин от файловых угроз с помощью политики (см. раздел "Создание политики" на стр. 141).

   Вы также можете создать и настроить задачи проверки для периодической проверки файлов виртуальных машин с использованием новых антивирусных баз (см. раздел "Проверка виртуальных машин" на стр. 154).

В этом разделе

Установка плагина Kaspersky Security для клиентов

Перед началом установки плагина управления Kaspersky Security для клиентов рекомендуется закрыть Консоль администрирования Kaspersky Security Center.
Установку плагина управления для клиентов следует выполнять под учетной записью, которая обладает правами на установку программного обеспечения (например, под учетной записью из группы локальных администраторов).

Плагин управления Kaspersky Security для клиентов должен быть установлен на том компьютере, где установлена Консоль администрирования Kaspersky Security Center.

► *Чтобы установить плагин управления Kaspersky Security для клиентов, выполните следующие действия:*

1. На компьютере, где установлена Консоль администрирования Kaspersky Security Center, запустите файл ksv-t-components_6.0.0.277_mlg.exe.

   Запустится мастер установки плагина управления Kaspersky Security для клиентов.

2. Выберите язык локализации мастера и плагина управления Kaspersky Security для клиентов и перейдите к следующему шагу мастера.

   По умолчанию в окне используется язык локализации операционной системы, установленной на компьютере, где запущен мастер.

3. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Для продолжения установки требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в окне мастера.

   Перейдите к следующему шагу мастера.

4. Просмотрите информацию о действиях, которые выполнит мастер, и нажмите на кнопку **Далее**, чтобы начать выполнение перечисленных действий.

5. Дождитесь завершения работы мастера.

   Если в ходе работы мастера возникает ошибка, мастер выполняет откат внесенных изменений.

6. Нажмите на кнопку **Завершить**, чтобы закрыть окно мастера.

Создание политики

► *Чтобы создать политику для клиентов, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.

2. В рабочей области выберите закладку **Политики** и нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики:

3. На первом шаге мастера в списке выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** и перейдите к следующему шагу мастера.

4. Введите название новой политики и перейдите к следующему шагу мастера.

5. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера.

   Мастер выполняет подключение к Серверу интеграции для получения информации о виртуальной инфраструктуре VMware.

   Мастер проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете

установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

6. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты. Значения параметров основного профиля защиты, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского".

   Основной профиль защиты назначается по умолчанию всем виртуальным машинам в составе защищаемой инфраструктуры.

   Значения параметров, установленные по умолчанию, достаточны для первоначальной настройки программы. Во время работы с программой вы можете выполнить более тонкую настройку параметров основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 144).

   Перейдите к следующему шагу мастера.

7. Примите решение об участии в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 168). Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

   - Если вы хотите использовать KSN в работе программы и согласны со всеми пунктами Положения, выберите вариант **Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network**.
   - Если вы не хотите принимать участие в KSN, выберите вариант **Я не принимаю условия настоящего Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

   При необходимости позже вы сможете изменить свое решение (см. раздел "Участие в Kaspersky Security Network" на стр. 168).

   > Параметры использования KSN (тип и режим использования KSN) определяются политикой провайдера, в области действия которой находятся виртуальные машины клиента.

   Перейдите к следующему шагу мастера.

8. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик в папке **Управляемые устройства** на закладке **Политики**.

Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе защищаемой инфраструктуры, вам нужно создать и назначить дополнительные профили защиты в свойствах политики (см. раздел "Назначение профиля защиты виртуальным машинам" на стр. 153).

kaspersky

Управление защитой от файловых угроз

Параметры, которые Kaspersky Security применяет во время защиты виртуальных машин, задаются с помощью политик (см. раздел "Создание политики" на стр. 141).

Kaspersky Security защищает только включенные виртуальные машины, которым назначен профиль защиты (см. раздел "Назначение профиля защиты виртуальным машинам" на стр. 153).

Когда пользователь или программа обращается к файлу виртуальной машины, Kaspersky Security проверяет этот файл.

- Если в файле не обнаружены вирусы или другие вредоносные программы, программа Kaspersky Security разрешает доступ к этому файлу.
- Если в файле обнаружены вирусы или другие вредоносные программы, программа Kaspersky Security присваивает файлу статус *Зараженный*. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или другим вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус *Зараженный*.

  После этого Kaspersky Security выполняет над файлом то действие, которое указано в профиле защиты этой виртуальной машины, например лечит или блокирует файл.

Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из защиты. Список исключений настраивается в параметрах профилей защиты.

Во время защиты виртуальных машин используется метод проверки *Сигнатурный анализ и машинное обучение*. Защита с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. Kaspersky Security использует базы программы, содержащие информацию об известных угрозах и о методах их устранения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Сигнатурный анализ и машинное обучение всегда включен.

Также во время защиты виртуальных машин используется *эвристический анализ* – это технология обнаружения угроз, которые невозможно определить с помощью баз программ "Лаборатории Касперского". Эвристический анализ позволяет находить файлы, которые, возможно, содержат вредоносную программу, не указанную в базах, или новую модификацию известного вируса. Файлам, в которых во время эвристического анализа обнаружена угроза, присваивается статус *Зараженный*.

Уровень эвристического анализа зависит от выбранного уровня безопасности:

- Если установлен уровень безопасности **Низкий**, применяется поверхностный уровень эвристического анализа. Эвристический анализатор выполняет не все инструкции исполняемых файлов во время проверки исполняемых файлов на наличие вредоносного кода. При таком уровне эвристического анализа вероятность обнаружить угрозу снижена по сравнению со средним уровнем эвристического анализа. Проверка требует меньше ресурсов SVM и проходит быстрее.
- Если установлен уровень безопасности **Рекомендуемый**, **Высокий** или **Пользовательский**, применяется средний уровень эвристического анализа. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет то количество инструкций в исполняемых файлах, которое рекомендовано специалистами "Лаборатории Касперского".

Информация обо всех событиях, произошедших во время защиты виртуальных машин, отправляется на Сервер администрирования Kaspersky Security Center.

Рекомендуется периодически просматривать список файлов, заблокированных в результате защиты виртуальных машин, и выполнять действия с этими файлами. Например, вы можете сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Информацию о заблокированных файлах вы можете просмотреть в выборке событий по событию *Файл заблокирован* (о событиях см. подробнее в документации Kaspersky Security Center).

Чтобы получить доступ к файлам, заблокированным в результате защиты виртуальных машин, требуется исключить эти файлы из защиты в параметрах профиля защиты, назначенного виртуальным машинам, или временно выключить защиту этих виртуальных машин (см. раздел "Выключение защиты виртуальных машин от файловых угроз" на стр. 154).

В этом разделе

Настройка параметров основного профиля защиты

Вы можете настроить параметры основного профиля защиты как во время создания политики (шаг **Настройка параметров основного профиля защиты**), так и в свойствах политики после ее создания (подраздел **Основной профиль защиты** в разделе **Защита от файловых угроз**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры основного профиля защиты, выполните следующие действия:*

1. В блоке **Уровень безопасности** выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины:
   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.

- Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка**. В открывшемся окне **Параметры уровня безопасности** выполните следующие действия:

a. В блоке **Проверка архивов и составных файлов** укажите значения следующих параметров:

- **Проверять архивы**

  Включение / выключение проверки архивов.

  По умолчанию флажок снят.

- **Удалять архивы, если лечение не удалось**

  Включение / выключение функции удаления архивов, лечение которых невозможно.

  Если флажок установлен, Kaspersky Security удаляет архивы, которые не удалось вылечить.

  Если флажок снят, программа не удаляет невылеченные архивы. Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию о том, что зараженный файл не удален.

  Флажок доступен для изменения, если установлен флажок **Проверять архивы**.

  По умолчанию флажок снят.

- **Проверять самораспаковывающиеся архивы**

  Включение / выключение проверки самораспаковывающихся архивов.

  По умолчанию для профилей защиты флажок снят, для задач проверки флажок установлен.

- **Проверять вложенные OLE-объекты**

  Включение / выключение проверки объектов, вложенных в файл.

  По умолчанию флажок установлен.

- **Не распаковывать составные файлы большого размера**

  Если флажок установлен, Kaspersky Security не проверяет составные файлы, размер которых превышает значение поля **Максимальный размер проверяемого составного файла N МБ**.

  Если флажок снят, Kaspersky Security проверяет составные файлы любого размера.

  Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

  По умолчанию флажок установлен.

- **Максимальный размер проверяемого составного файла N МБ**

  Максимальный размер составных файлов, подлежащих проверке (в мегабайтах). Kaspersky Security не распаковывает и не проверяет те объекты, размер которых больше указанного значения.

  Параметр доступен для изменения, если установлен флажок **Не распаковывать составные файлы большого размера**.

  Вы можете указать в этом поле значение от 1 до 999999. По умолчанию задано значение 8 МБ.

b. В блоке **Производительность** укажите значения следующих параметров:

- **Ограничивать время проверки файлов**

  Включение / выключение ограничения времени проверки файлов.

  Если флажок установлен, Kaspersky Security прекращает проверку файла, если время проверки достигает значения, заданного в поле **Проверять файлы не дольше N секунд(ы)**, и пропускает этот файл.

  Если флажок снят, Kaspersky Security не ограничивает время проверки файлов.

  По умолчанию для профилей защиты флажок установлен, для задач проверки флажок снят.

- **Проверять файлы не дольше N секунд(ы)**

  Максимальная длительность проверки файла (в секундах). Kaspersky Security прекращает проверку файла, если она длится больше заданного значения времени.

  Параметр доступен для изменения, если установлен флажок **Ограничивать время проверки файлов**.

  Вы можете указать в этом поле значение от 1 до 3600. По умолчанию задано значение 60 секунд.

c. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка** и укажите в открывшемся окне **Объекты для обнаружения** значения следующих параметров:

- **Вредоносные утилиты**

  Включение / выключение защиты от вредоносных утилит.

  Вредоносные утилиты не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на виртуальной машине. Злоумышленники используют функции вредоносных утилит для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы или других вредоносных действий.

  Если флажок установлен, защита от вредоносных утилит включена.

  Если флажок снят, защита от вредоносных утилит выключена.

  По умолчанию флажок установлен.

- **Программы автодозвона**

  Включение / выключение защиты от программ автодозвона.

  Если флажок установлен, защита от программ автодозвона включена.

  Если флажок снят, защита от программ автодозвона выключена.

  По умолчанию флажок установлен.

- **Рекламные программы**

  Включение / выключение защиты от рекламных программ.

  Рекламные программы связаны с показом пользователю рекламной информации, например: отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-сайты. Некоторые из рекламных программ собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов рекламные программы передают эту информацию разработчику с разрешения пользователя.

Если флажок установлен, защита от рекламных программ включена.

Если флажок снят, защита от рекламных программ выключена.

По умолчанию флажок установлен.

- **Другие**

  Включение / выключение защиты от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя.

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ находятся IRC-клиенты, программы для загрузки файлов, программы удаленного администрирования, программы для отслеживания действий пользователя, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet. Однако если злоумышленники получат доступ к таким программам, они могут использовать некоторые их функции для нанесения вреда виртуальной машине или данным пользователя.

  Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя, включена.

  Если флажок снят, защита от таких программ выключена.

  По умолчанию флажок снят.

- **Многократно упакованные файлы**

  Включение / выключение проверки файлов, которые упакованы одним или несколькими упаковщиками три или более раз.

  Если файл упакован одним или несколькими упаковщиками три или более раз, то существует вероятность, что файл содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Если флажок установлен, защита от многократно упакованных файлов включена, и проверка таких файлов разрешена.

  Если флажок снят, защита от многократно упакованных файлов выключена.

  По умолчанию флажок установлен.

  > Kaspersky Security всегда проверяет файлы виртуальных машин на наличие вирусов, червей и троянских программ. Поэтому параметры **Вирусы и черви** и **Троянские программы** в блоке **Вредоносные программы** недоступны для изменения.

d. Нажмите на кнопку **ОК** в окне **Объекты для обнаружения**.

e. Нажмите на кнопку **ОК** в окне **Параметры уровня безопасности**.

   Если вы изменили параметры уровня безопасности, программа создаст пользовательский уровень безопасности. Название уровня безопасности в блоке **Уровень безопасности** изменится на **Пользовательский**.

2. В блоке **Действие при обнаружении угрозы** выберите действие в раскрывающемся списке.

   Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов:

- **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.
- **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

  Это действие выбрано по умолчанию.

  Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить, только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.
- **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.
- **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

3. Если вы хотите, чтобы во время защиты виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяла файлы на сетевых дисках, снимите флажок **Проверять сетевые диски** в блоке **Область защиты**. По умолчанию во время защиты виртуальных машин с операционными системами Windows программа проверяет на сетевых дисках все файлы, для которых не настроено исключение из защиты.

   Во время защиты виртуальных машин с операционными системами Linux программа Kaspersky Security всегда проверяет файлы поддерживаемых сетевых файловых систем (NFS и CIFS). Если вы хотите исключить из области защиты файлы сетевых файловых систем, вам требуется настроить исключение из защиты для директории, в которую смонтирована сетевая файловая система.

   > Kaspersky Security всегда проверяет файлы на съемных и жестких дисках. Поэтому параметр **Проверять все съемные и жесткие диски** в блоке **Область защиты** недоступен для изменения.

4. Если вы хотите исключить из защиты какие-либо файлы виртуальных машин, нажмите на кнопку **Настройка** в блоке **Исключения из защиты**.

   В открывшемся окне **Исключения из защиты** укажите следующие параметры:

   a. В блоке **Расширения файлов** выберите один из следующих вариантов:

      - **Проверять все, кроме файлов со следующими расширениями**. В поле ввода укажите список расширений файлов, которые не надо проверять во время защиты виртуальной машины. Kaspersky Security не учитывает регистр символов в расширениях файлов, которые требуется исключить из области защиты.
      - **Проверять только файлы со следующими расширениями**. В поле ввода укажите список расширений файлов, которые надо проверять во время защиты виртуальной машины. Во время защиты виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в расширениях файлов, которые требуется включить в область защиты. Во время защиты виртуальных машин с операционными системами Windows регистр символов в расширениях файлов не учитывается.

      Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении

используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

> Если вы выбрали в раскрывающемся списке вариант **Проверять только файлы со следующими расширениями**, но не указали расширения файлов, которые надо проверять, Kaspersky Security проверяет все файлы.

b. В таблице **Папки и файлы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список объектов, которые требуется исключить из защиты.

По умолчанию список исключений содержит объекты, рекомендуемые корпорацией Microsoft (список рекомендуемых исключений см. на сайте корпорации Microsoft). Kaspersky Security исключает эти объекты из защиты на всех виртуальных машинах, которым назначен основной профиль защиты. Вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы**.

Вы можете исключать из защиты объекты следующих типов:

- Папки. Из защиты исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение из защиты к вложенным папкам.
- Файлы по маске. Из защиты исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

  При указании маски файла вы можете использовать символы `*` и `?`.

Программа Kaspersky Security игнорирует регистр символов в путях к файлам и папкам, исключаемым из защиты.

Вы можете сохранить настроенный список исключений в файле с помощью кнопки **Экспорт** и загрузить ранее сохраненный список исключений из файла с помощью кнопки **Импорт**. Для импорта и экспорта списка исключений вы можете использовать файл в формате XML. Импортировать список исключений вы также можете из файла в формате DAT. С помощью файла в формате DAT вы можете импортировать список исключений, сформированный в других программах "Лаборатории Касперского".

> Если вы используете в списке исключений переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows из защиты исключаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, из защиты исключаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

5. Нажмите на кнопку **ОК** в окне **Исключения из защиты**.
6. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания политики) или на кнопку **Применить** (в свойствах политики).

Измененные параметры профиля защиты вступят в силу после синхронизации данных между программой Kaspersky Security Center и SVM.

Управление дополнительными профилями защиты

Вы можете управлять дополнительными профилями защиты в свойствах политики в списке дополнительных профилей защиты.

► *Чтобы открыть список дополнительных профилей защиты в свойствах политики, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Политики**.
3. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
4. В окне свойств политики в разделе **Защита от файловых угроз** выберите подраздел **Дополнительные профили защиты**.

   В правой части окна отобразится список дополнительных профилей защиты. Если вы еще не создавали дополнительные профили защиты в этой политике, то список профилей защиты пуст.

В списке дополнительных профилей защиты вы можете выполнять следующие действия:

- Создавать дополнительные профили защиты (см. раздел "Создание дополнительного профиля защиты" на стр. 150).
- Изменять имя дополнительного профиля защиты по кнопке **Переименовать**.
- Изменять параметры дополнительных профилей защиты по кнопке **Изменить**. Изменение параметров выполняется в окне **Параметры защиты**. Параметры дополнительного профиля защиты аналогичны параметрам основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 144).
- Экспортировать параметры дополнительного профиля защиты в файл по кнопке **Экспорт**. Для сохранения параметров дополнительного профиля защиты нужно указать путь к файлу в формате JSON. Ранее сохраненные параметры вы можете использовать при создании нового дополнительного профиля защиты (см. раздел "Создание дополнительного профиля защиты" на стр. 150).
- Удалять дополнительные профили защиты по кнопке **Удалить**. Если этот профиль защиты использовался для защиты виртуальных машин, программа будет защищать эти виртуальные машины с параметрами профиля защиты, который назначен их родительскому объекту в виртуальной инфраструктуре. Если родительский объект исключен из защиты, программа не будет защищать эти виртуальные машины.

Создание дополнительного профиля защиты

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы создать дополнительный профиль защиты, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте список дополнительных профилей защиты в свойствах политики, для которой вы хотите создать дополнительный профиль защиты (см. раздел "Управление дополнительными профилями защиты" на стр. 150).
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Профиль защиты**.
3. В открывшемся окне введите имя нового профиля защиты.

   Имя профиля защиты не может содержать более 255 символов.
4. Если при создании нового профиля защиты вы хотите использовать ранее сохраненные параметры профиля защиты, установите флажок **Импортировать параметры из файла** и укажите путь к файлу в формате JSON.
5. Нажмите на кнопку **ОК** в окне **Профиль защиты**.

   Откроется окно **Параметры защиты**. В этом окне вы можете настроить параметры нового профиля защиты или изменить параметры профиля защиты, импортированные из файла.

   Параметры дополнительного профиля защиты, кроме списка исключений по умолчанию, аналогичны параметрам основного профиля защиты (см. раздел "Настройка параметров основного профиля защиты" на стр. 144).

   Список исключений по умолчанию не содержит объекты, рекомендуемые корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Если вы хотите, чтобы объекты, рекомендуемые корпорацией Microsoft, исключались из защиты на всех виртуальных машинах, которым назначен этот профиль защиты, вам нужно импортировать в исключения профиля защиты файл microsoft_file_exclusions.xml.
   Файл microsoft_file_exclusions.xml входит в комплект поставки программы и расположен в папке установки плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. После импортирования вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы** в окне **Исключения из защиты**.
6. После настройки всех параметров профиля защиты нажмите на кнопку **ОК** в окне **Параметры защиты**.

   В окне **Свойства: <Название политики>** в списке дополнительных профилей защиты отобразится новый профиль защиты.

Созданный профиль защиты вы можете назначить виртуальным машинам (см. раздел "Назначение профиля защиты виртуальным машинам" на стр. 153).

Просмотр защищаемой инфраструктуры в политике

В свойствах политики вы можете посмотреть защищаемую инфраструктуру, выбранную для политики, и информацию об использовании профилей защиты.

► *Чтобы просмотреть информацию о защищаемой инфраструктуре в политике, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики:
   a. В дереве консоли выберите папку **Управляемые устройства**.
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики в разделе **Защита от файловых угроз** выберите подраздел **Защищаемая инфраструктура**.

   Плагин управления Kaspersky Security пытается автоматически подключиться к Серверу интеграции. Если установить подключение не удалось, откроется окно **Подключение к Серверу интеграции**. Укажите адрес Сервера интеграции и нажмите на кнопку **ОК** в окне **Подключение к Серверу интеграции**.
3. Плагин управления Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

   Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

После подключения к Серверу интеграции в правой части окна отображается информация о защищаемой инфраструктуре и использовании профилей защиты.

Информация о защищаемой инфраструктуре

Защищаемая инфраструктура отображается в виде дерева элементов. Корневым элементом является условный объект «Организация vCloud Director», который объединяет все виртуальные Datacenter вашей виртуальной инфраструктуры.

Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если этой

виртуальной машине назначен профиль защиты, параметры этого профиля защиты применяются ко всем виртуальным машинам, которые имеют одинаковый идентификатор (vmID).

Информация о назначении профилей защиты объектам виртуальной инфраструктуры

В графе **Профиль защиты** отображается информация о назначении объектам защищаемой инфраструктуры профилей защиты. Параметры назначенных профилей защиты Kaspersky Security использует во время защиты виртуальных машин.

Информация отображается следующим образом:

- Название назначенного явно профиля защиты выделяется черным цветом.
- Название унаследованного от родительского объекта профиля защиты выделяется серым цветом. Название формируется следующим образом: "унаследованный: <N>", где <N> – название унаследованного от родительского объекта профиля защиты.
- Если объекту защищаемой инфраструктуры профиль защиты не назначен (объект исключен из защиты), в графе **Профиль защиты** отображается значение *(Не назначен)*.

По умолчанию основной профиль защиты назначен корневому объекту "Организация vCloud Director" и наследуется всеми объектами виртуальной инфраструктуры.

Назначение профиля защиты виртуальным машинам

► *Чтобы назначить виртуальным машинам профиль защиты, выполните следующие действия:*

1. В свойствах политики выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 152).
2. Выберите в таблице одну или несколько виртуальных машин.

   Если вы хотите назначить одинаковый профиль защиты всем виртуальным машинам, которые являются дочерними объектами одного виртуального Datacenter, выберите в таблице этот Datacenter. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.
3. Нажмите на кнопку **Выбрать профиль защиты**.

   Откроется окно **Выбор профиля защиты**.
4. Выберите один из следующих вариантов:
   - **Наследовать родительский профиль защиты: <имя>**. Выберите этот вариант, чтобы назначить виртуальной машине или другому объекту виртуальной инфраструктуры профиль защиты родительского объекта.
   - **Использовать профиль защиты**. Выберите этот вариант и укажите в раскрывающемся списке имя профиля защиты, чтобы назначить этот профиль защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.
5. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, профиль защиты назначается объекту и всем его дочерним объектам, включая объекты, которым назначен собственный профиль защиты или которые исключены из защиты. Если вы хотите назначить профиль защиты только выбранному объекту виртуальной инфраструктуры и тем его дочерним объектам, которые наследуют профиль защиты и которые не исключены из защиты, снимите флажок **Применить ко всем дочерним объектам**.

6. Нажмите на кнопку **ОК**.

   Окно **Выбор профиля защиты** закроется, назначенный профиль защиты отобразится в таблице в подразделе **Защищаемая инфраструктура**.

7. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Выключение защиты виртуальных машин от файловых угроз

Выключение функции защиты приводит к выходу программы из сертифицированного состояния.

► *Чтобы выключить защиту виртуальных машин, выполните следующие действия:*

1. В свойствах политики выберите подраздел **Защищаемая инфраструктура** (см. раздел "**Просмотр защищаемой инфраструктуры в политике**" на стр. 152).
2. Если вы хотите выключить защиту для одной или нескольких виртуальных машин, выполните следующие действия:
   a. Выберите в таблице одну или несколько виртуальных машин.

      Если вы хотите выключить защиту для всех виртуальных машин, которые являются дочерними объектами одного виртуального Datacenter, выберите в таблице этот Datacenter. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.

   b. Нажмите на кнопку **Выбрать профиль защиты**.

      Откроется окно **Выбор профиля защиты**.

   c. Выберите вариант **Не использовать профиль защиты**.

   d. Если вы выбрали Datacenter, по умолчанию защита будет выключена для всех виртуальных машин в его составе, включая виртуальные машины, которым назначен собственный профиль защиты. Если вы хотите выключить защиту только для тех виртуальных машин, которые наследуют профиль защиты от родительского объекта, снимите флажок **Применить ко всем дочерним объектам**.

   e. Нажмите на кнопку **ОК**.

      Окно **Выбор профиля защиты** закроется, в таблице в подразделе **Защищаемая инфраструктура** для виртуальных машин, которые исключены из защиты, в графе **Профиль защиты** отобразится значение *(Не назначен)*.

3. Если вы хотите выключить защиту для всех виртуальных машин в вашей виртуальной инфраструктуре, снимите флажок **Использовать защиту от файловых угроз**, расположенный в верхней части окна.
4. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Проверка виртуальных машин

Kaspersky Security позволяет выполнять антивирусную проверку файлов виртуальных машин на гипервизоре VMware ESXi. Требуется периодически проверять файлы виртуальных машин с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов.

Параметры, которые Kaspersky Security применяет во время проверки виртуальных машин, задаются с помощью задач проверки. Kaspersky Security использует для проверки следующие задачи:

- **Полная проверка**. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин в вашей виртуальной инфраструктуре.
- **Выборочная проверка**. Задача позволяет выполнять антивирусную проверку файлов тех виртуальных машин, которые вы указали в параметрах задачи. Вы можете указывать отдельные виртуальные машины или объекты виртуальной инфраструктуры VMware более высокого уровня иерархии.

Вы можете задавать расписание выполнения задач проверки, запускать задачи проверки вручную и просматривать информацию о ходе и результатах выполнения задач (см. раздел "О задачах" на стр. 138).

Если во время проверки файлов виртуальных машин в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус *Зараженный*. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус *Зараженный*.

При проверке виртуальных машин используется метод проверки *Сигнатурный анализ и машинное обучение*. Проверка с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. Kaspersky Security использует базы программы, содержащие информацию об известных угрозах и о методах их устранения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Сигнатурный анализ и машинное обучение всегда включен.

Также при проверке виртуальных машин используется *эвристический анализ* – это технология обнаружения угроз, которые невозможно определить с помощью баз программ "Лаборатории Касперского". Эвристический анализ позволяет находить файлы, которые, возможно, содержат вредоносную программу, не указанную в базах, или новую модификацию известного вируса. Файлам, в которых во время эвристического анализа обнаружена угроза, присваивается статус *Зараженный*.

Во время проверки виртуальных машин всегда используется глубокий уровень эвристического анализа независимо от выбранного уровня безопасности. Эвристический анализатор выполняет максимальное количество инструкций в исполняемых файлах, что позволяет повысить вероятность обнаружения угрозы.

Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из области проверки.

Особенности проверки виртуальных машин:

- При выполнении задач проверки Kaspersky Security может проверять выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS.
- При выполнении задач проверки Kaspersky Security может проверять шаблоны виртуальных машин.
- При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется настроить задачу проверки для виртуальных машин, на которых открыт сетевой доступ к папкам и файлам, и включить эти папки и файлы в область проверки задачи.

  При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы

сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

После завершения задачи проверки рекомендуется просмотреть список файлов, заблокированных в результате выполнения задачи, и вручную выполнить действия с этими файлами. Например, сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Предварительно требуется исключить заблокированные файлы из защиты в параметрах профиля защиты, назначенного виртуальным машинам, или временно выключить защиту виртуальных машин, на которых были заблокированы эти файлы (см. раздел "Выключение защиты виртуальных машин от файловых угроз" на стр. 154). Информацию о заблокированных файлах вы можете просмотреть в выборке событий по событию *Файл заблокирован* (см. в документации Kaspersky Security Center).

В этом разделе

Создание задачи полной проверки

► *Чтобы создать задачу полной проверки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
3. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** → **Полная проверка**.

   Перейдите к следующему шагу мастера создания задачи.
4. Настройте параметры проверки виртуальных машин (см. раздел "Настройка параметров проверки виртуальных машин в задаче проверки" на стр. 160).

   Перейдите к следующему шагу мастера создания задачи.
5. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи (см. раздел "Настройка области проверки в задаче проверки" на стр. 165).

   Перейдите к следующему шагу мастера создания задачи.
6. Чтобы настроить расписание запуска задачи, определите значения следующих параметров:
   - **Запуск по расписанию**. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.
   - **Запускать пропущенные задачи**. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов **Вручную** и **Один раз** задача запускается сразу после появления SVM в сети.

Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов **Вручную** и **Один раз** – только на видимых в сети SVM.

- **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:
  - 0–200 SVM – запуск задачи не распределяется;
  - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
  - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
  - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
  - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
  - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
  - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
  - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
  - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

  Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию флажок установлен.
- **Использовать случайную задержку запуска задачи в интервале (мин)**. Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

  Распределенный запуск задачи помогает избежать одновременного обращения большого количества SVM к Серверу администрирования Kaspersky Security Center.

Перейдите к следующему шагу мастера создания задачи.

7. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера создания задачи.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

   Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную (см. раздел "О задачах" на стр. 138).

Создание задачи выборочной проверки

► *Чтобы создать задачу выборочной проверки для виртуальных машин клиентов, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства** виртуального Сервера администрирования, соответствующего клиенту.

2. В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
3. На первом шаге мастера выберите **Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов)** → **Выборочная проверка**.

   Перейдите к следующему шагу мастера создания задачи.
4. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера создания задачи.

   Мастер создания задачи проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. SSL-сертификат используется для установки защищенного соединения с Сервером интеграции. При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных. Чтобы посмотреть информацию о полученном сертификате, нажмите на кнопку **Посмотреть полученный сертификат** в окне с сообщением об ошибке. Вы можете установить полученный сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**.

   Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center. При этом выполняется проверка ранее установленного доверенного сертификата для этого Сервера интеграции. Если полученный сертификат не соответствует ранее установленному сертификату, откроется окно для подтверждения замены ранее установленного сертификата. Чтобы заменить ранее установленный сертификат на сертификат, полученный от Сервера интеграции, и продолжить подключение, нажмите на кнопку **Да** в этом окне.
5. Выберите область действия задачи: установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

   > Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

   Перейдите к следующему шагу мастера создания задачи.
6. Настройте параметры проверки виртуальных машин (см. раздел "Настройка параметров проверки виртуальных машин в задаче проверки" на стр. 160).

   Перейдите к следующему шагу мастера создания задачи.
7. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи (см. раздел "Настройка области проверки в задаче проверки" на стр. 165).

   Перейдите к следующему шагу мастера создания задачи.
8. Чтобы настроить расписание запуска задачи, определите значения следующих параметров:

   - **Запуск по расписанию**. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Запускать пропущенные задачи**. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов **Вручную** и **Один раз** задача запускается сразу после появления SVM в сети.

  Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов **Вручную** и **Один раз** – только на видимых в сети SVM.

- **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию запуск задачи на SVM распределяется в течение определенного периода времени. Этот период рассчитывается автоматически, в зависимости от количества SVM, на которые распространяется задача:

  - 0–200 SVM – запуск задачи не распределяется;
  - 200–500 SVM – запуск задачи распределяется в течение 5 минут;
  - 500–1000 SVM – запуск задачи распределяется в течение 10 минут;
  - 1000–2000 SVM – запуск задачи распределяется в течение 15 минут;
  - 2000–5000 SVM – запуск задачи распределяется в течение 20 минут;
  - 5000–10000 SVM – запуск задачи распределяется в течение 30 минут;
  - 10000–20000 SVM – запуск задачи распределяется в течение 1 часа;
  - 20000–50000 SVM – запуск задачи распределяется в течение 2 часов;
  - более 50000 SVM – запуск задачи распределяется в течение 3 часов.

  Если не требуется распределять запуск задачи в течение автоматически рассчитываемого периода, снимите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**. По умолчанию флажок установлен.

- **Использовать случайную задержку запуска задачи в интервале (мин)**. Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

  Распределенный запуск задачи помогает избежать одновременного обращения большого количества SVM к Серверу администрирования Kaspersky Security Center.

Перейдите к следующему шагу мастера создания задачи.

9. В поле **Имя** введите название задачи и перейдите к следующему шагу мастера создания задачи.
10. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

    Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную (см. раздел "О задачах" на стр. 138).

kaspersky

Настройка параметров проверки виртуальных машин в задаче проверки

Вы можете настроить параметры проверки виртуальных машин во время создания задачи (шаг **Настройка параметров проверки**) или в свойствах задачи после ее создания (раздел **Параметры проверки**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить параметры проверки виртуальных машин, выполните следующие действия:*

1. Выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины. Для этого в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его с помощью ползунка.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка**. В открывшемся окне **Параметры уровня безопасности** выполните следующие действия:

   a. В блоке **Проверка архивов и составных файлов** укажите значения следующих параметров:

   - **Проверять архивы**

     Включение / выключение проверки архивов.

     По умолчанию флажок снят.

   - **Удалять архивы, если лечение не удалось**

     Включение / выключение функции удаления архивов, лечение которых невозможно.

     Если флажок установлен, Kaspersky Security удаляет архивы, которые не удалось вылечить.

     Если флажок снят, программа не удаляет невылеченные архивы. Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию о том, что зараженный файл не удален.

     Флажок доступен для изменения, если установлен флажок **Проверять архивы**.

     По умолчанию флажок снят.

   - **Проверять самораспаковывающиеся архивы**

Включение / выключение проверки самораспаковывающихся архивов.

По умолчанию для профилей защиты флажок снят, для задач проверки флажок установлен.

- **Проверять вложенные OLE-объекты**

  Включение / выключение проверки объектов, вложенных в файл.

  По умолчанию флажок установлен.

- **Не распаковывать составные файлы большого размера**

  Если флажок установлен, Kaspersky Security не проверяет составные файлы, размер которых превышает значение поля **Максимальный размер проверяемого составного файла N МБ**.

  Если флажок снят, Kaspersky Security проверяет составные файлы любого размера.

  Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

  По умолчанию флажок установлен.

- **Максимальный размер проверяемого составного файла N МБ**

  Максимальный размер составных файлов, подлежащих проверке (в мегабайтах). Kaspersky Security не распаковывает и не проверяет те объекты, размер которых больше указанного значения.

  Параметр доступен для изменения, если установлен флажок **Не распаковывать составные файлы большого размера**.

  Вы можете указать в этом поле значение от 1 до 999999. По умолчанию задано значение 8 МБ.

b. В блоке **Производительность** укажите значения следующих параметров:

- **Ограничивать время проверки файлов**

  Включение / выключение ограничения времени проверки файлов.

  Если флажок установлен, Kaspersky Security прекращает проверку файла, если время проверки достигает значения, заданного в поле **Проверять файлы не дольше N секунд(ы)**, и пропускает этот файл.

  Если флажок снят, Kaspersky Security не ограничивает время проверки файлов.

  По умолчанию для профилей защиты флажок установлен, для задач проверки флажок снят.

- **Проверять файлы не дольше N секунд(ы)**

  Максимальная длительность проверки файла (в секундах). Kaspersky Security прекращает проверку файла, если она длится больше заданного значения времени.

  Параметр доступен для изменения, если установлен флажок **Ограничивать время проверки файлов**.

  Вы можете указать в этом поле значение от 1 до 3600. По умолчанию задано значение 60 секунд.

c. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка** и укажите в открывшемся окне **Объекты для обнаружения** значения следующих параметров:

- **Вредоносные утилиты**

  Включение / выключение защиты от вредоносных утилит.

  Вредоносные утилиты не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на виртуальной машине. Злоумышленники используют функции вредоносных утилит для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы или других вредоносных действий.

  Если флажок установлен, защита от вредоносных утилит включена.

  Если флажок снят, защита от вредоносных утилит выключена.

  По умолчанию флажок установлен.

- **Программы автодозвона**

  Включение / выключение защиты от программ автодозвона.

  Если флажок установлен, защита от программ автодозвона включена.

  Если флажок снят, защита от программ автодозвона выключена.

  По умолчанию флажок установлен.

- **Рекламные программы**

  Включение / выключение защиты от рекламных программ.

  Рекламные программы связаны с показом пользователю рекламной информации, например: отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-сайты. Некоторые из рекламных программ собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов рекламные программы передают эту информацию разработчику с разрешения пользователя.

  Если флажок установлен, защита от рекламных программ включена.

  Если флажок снят, защита от рекламных программ выключена.

  По умолчанию флажок установлен.

- **Другие**

  Включение / выключение защиты от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя.

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ находятся IRC-клиенты, программы для загрузки файлов, программы удаленного администрирования, программы для отслеживания действий пользователя, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet. Однако если злоумышленники получат доступ к таким программам, они могут использовать некоторые их функции для нанесения вреда виртуальной машине или данным пользователя.

  Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда виртуальной машине или данным пользователя, включена.

  Если флажок снят, защита от таких программ выключена.

  По умолчанию флажок снят.

- **Многократно упакованные файлы**

  Включение / выключение проверки файлов, которые упакованы одним или несколькими упаковщиками три или более раз.

  Если файл упакован одним или несколькими упаковщиками три или более раз, то существует вероятность, что файл содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Если флажок установлен, защита от многократно упакованных файлов включена, и проверка таких файлов разрешена.

  Если флажок снят, защита от многократно упакованных файлов выключена.

  По умолчанию флажок установлен.

> Kaspersky Security всегда проверяет файлы виртуальных машин на наличие вирусов, червей и троянских программ. Поэтому параметры **Вирусы и черви** и **Троянские программы** в блоке **Вредоносные программы** недоступны для изменения.

d. Нажмите на кнопку **ОК** в окне **Объекты для обнаружения**.

e. Нажмите на кнопку **ОК** в окне **Параметры уровня безопасности**.

   Если вы изменили параметры уровня безопасности, программа создаст пользовательский уровень безопасности. Название уровня безопасности в блоке **Уровень безопасности** изменится на **Пользовательский**.

2. В блоке **Проверка включенных виртуальных машин** настройте параметры проверки виртуальных машин, которые включены во время выполнения задачи:

   - **Действие при обнаружении угрозы**

     Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов на включенных виртуальных машинах:

     - **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.
     - **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

       Это действие выбрано по умолчанию.

       Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить, только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.
     - **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.
     - **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

   - **Проверять оптические диски**

     Включение / выключение проверки оптических дисков.

Если флажок установлен, Kaspersky Security проверяет файлы на оптических дисках (CD, DVD, Blu-Ray) при выполнении задачи проверки на виртуальных машинах с операционными системами Windows.

Если флажок снят, Kaspersky Security не проверяет файлы на оптических дисках.

Если флажок установлен, но для задачи задана область проверки, в которую не включен путь к оптическому диску, Kaspersky Security не проверяет файлы на оптическом диске.

Kaspersky Security не проверяет файлы на оптических дисках при проверке выключенных виртуальных машин, шаблонов виртуальных машин и виртуальных машин с операционными системами Linux.

По умолчанию флажок снят.

3. В блоке **Проверка выключенных виртуальных машин и шаблонов виртуальных машин** настройте параметры проверки виртуальных машин, которые выключены или приостановлены во время выполнения задачи, а также шаблонов виртуальных машин:

   - **Проверять выключенные виртуальные машины**

     Включение / выключение проверки выключенных виртуальных машин.

     Если флажок установлен, при выполнении задачи проверки Kaspersky Security проверяет файлы на выключенных виртуальных машинах, входящих в область действия задачи, с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS. Файлы на выключенных виртуальных машинах с другими файловыми системами не проверяются.

     Во время проверки выключенную виртуальную машину невозможно включить или выполнить ее миграцию.

     Если флажок снят, Kaspersky Security не проверяет файлы на выключенных виртуальных машинах.

     По умолчанию флажок снят.

   - **Проверять шаблоны виртуальных машин**

     Включение / выключение проверки шаблонов виртуальных машин.

     Если флажок установлен, при выполнении задачи проверки Kaspersky Security проверяет файлы на шаблонах виртуальных машин, входящих в область действия задачи.

     Если флажок снят, Kaspersky Security не проверяет файлы на шаблонах виртуальных машин.

     По умолчанию флажок снят.

     Флажок доступен, если установлен флажок **Проверять выключенные виртуальные машины**.

   - **Действие при обнаружении угрозы**

     Раскрывающийся список содержит действия, которые может выполнять Kaspersky Security при обнаружении зараженных файлов на выключенных виртуальных машинах или шаблонах виртуальных машин:

     - **Лечить. Блокировать, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, Kaspersky Security блокирует эти файлы.
     - **Лечить. Удалять, если лечение невозможно**. Kaspersky Security автоматически пытается вылечить зараженные файлы. Если лечение невозможно, программа

удаляет эти файлы. Если удаление невозможно, Kaspersky Security блокирует зараженные файлы.

Kaspersky Security удаляет зараженные архивы, которые не удалось вылечить, только если в параметрах уровня безопасности установлен флажок **Удалять архивы, если лечение не удалось**.

- **Удалять. Блокировать, если удаление невозможно**. Kaspersky Security автоматически удаляет зараженные файлы без попытки их вылечить. Если удаление невозможно, Kaspersky Security блокирует эти файлы.
- **Блокировать**. Kaspersky Security автоматически блокирует зараженные файлы без попытки их вылечить.

  Это действие выбрано по умолчанию.

Выбор действия доступен, если установлен флажок **Проверять выключенные виртуальные машины**.

4. В блоке **Останавливать проверку** выберите один из следующих вариантов:
   - **По истечении N минут(ы) с момента запуска задачи**

     Максимальное время выполнения задачи проверки (в минутах). По достижении заданного времени выполнение задачи проверки прекращается, даже если проверка не была завершена.

     Этот вариант выбран по умолчанию.

     Вы можете указать в этом поле значение от 1 до 4320. По умолчанию указано значение 120 минут.
   - **После окончания проверки файлов на всех защищенных виртуальных машинах**

     Задача проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах, входящих в область действия задачи.
5. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Настройка области проверки в задаче проверки

Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Если область проверки не настроена, Kaspersky Security проверяет все файлы виртуальных машин.

При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется создать задачу проверки виртуальных машин, папки и файлы которых открыты для сетевого доступа, и включить эти папки и файлы в область проверки задачи.

При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

Вы можете сформировать область проверки задачи во время создания задачи (шаг **Выбор области проверки**) или в свойствах задачи после ее создания (раздел **Область проверки**).

Изменение значений некоторых параметров программы может привести к выходу программы из сертифицированного состояния. Описание параметров, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии приведено в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 178).

Не рекомендуется устанавливать значения параметров ниже заданных по умолчанию, так как это негативно влияет на безопасное использование программы.

► *Чтобы настроить область проверки задачи, выполните следующие действия:*

1. Выберите один из следующих вариантов:
   - **Проверять все папки и файлы, кроме указанных**.
   - **Проверять только указанные папки и файлы**.
2. Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, вы можете сформировать список объектов, которые требуется исключить из области проверки, с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

   Вы можете исключать из области проверки объекты следующих типов:

   - Папки. Из области проверки исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение к вложенным папкам.
   - Файлы по маске. Из области проверки исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

     При указании маски файла вы можете использовать символы `*` и `?`.

     Kaspersky Security не учитывает регистр символов в путях к файлам и папкам, именах и масках файлов, которые требуется исключить из области проверки.

   Вы можете сохранить настроенный список исключений в файл с помощью кнопки **Экспорт** и загрузить ранее сохраненный список исключений из файла с помощью кнопки **Импорт**. Для импорта и экспорта списка исключений вы можете использовать файл в формате XML. Импортировать список исключений вы также можете из файла в формате DAT. С помощью файла в формате DAT вы можете импортировать список исключений, сформированный в других программах "Лаборатории Касперского".

   В комплект поставки программы входит файл microsoft_file_exclusions.xml, который содержит список исключений, рекомендуемых корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Файл microsoft_file_exclusions.xml расположен в папке установки

плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Вы можете импортировать этот файл в исключения задачи проверки. После выполнения импорта Kaspersky Security не проверяет объекты, рекомендуемые корпорацией Microsoft, во время выполнения задачи проверки. Вы можете просмотреть и изменить список этих объектов в таблице **Папки и файлы**.

Если вы используете в списке исключений переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows из области проверки исключаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, из области проверки исключаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

3. Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, в блоке **Расширения файлов** вы можете указать расширения файлов, которые нужно включить в область проверки или исключить из области проверки.

   Для этого выберите один из следующих вариантов:

   - **Проверять все, кроме файлов со следующими расширениями**. В поле ввода укажите список расширений файлов, которые не надо проверять во время выполнения задачи проверки. Kaspersky Security не учитывает регистр символов в расширениях файлов, которые требуется исключить из области проверки.
   - **Проверять только файлы со следующими расширениями**. В поле ввода укажите список расширений файлов, которые надо проверять во время выполнения задачи проверки. При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в расширениях файлов, которые требуется включить в область проверки. При проверке виртуальных машин с операционными системами Windows регистр символов в расширениях файлов не учитывается.

     Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

     Если вы выбрали в раскрывающемся списке вариант **Проверять только файлы со следующими расширениями**, но не указали расширения файлов, которые надо проверять, Kaspersky Security проверяет все файлы.

   Исключенные из проверки папки имеют более высокий приоритет, чем расширения файлов, включенные в область проверки. Если файл находится в папке, исключенной из проверки, то программа не проверяет его, несмотря на то, что расширение файла включено в область проверки.

4. Если вы выбрали вариант **Проверять только указанные папки и файлы**, с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список папок и файлов на виртуальной машине, которые нужно проверять во время выполнения задачи проверки.

   При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в путях к файлам и директориям, включаемым в область проверки. При

проверке виртуальных машин с операционными системами Windows регистр символов в путях к файлам и папкам не учитывается.

> Если в списке объектов, которые нужно проверять, вы используете переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows в область проверки включаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, в область проверки включаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

5. Сохраните внесенные изменения, нажав на кнопку **Далее** (в мастере создания задачи) или на кнопку **Применить** (в свойствах задачи).

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальных машин, Kaspersky Security может использовать данные, полученные от пользователей программ "Лаборатории Касперского" во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Если вы участвуете в Kaspersky Security Network, программа Kaspersky Security получает от служб KSN сведения о категории и репутации проверяемых файлов.

В зависимости от расположения инфраструктуры KSN различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского". Если вы используете Глобальный KSN, Kaspersky Security автоматически отправляет в "Лабораторию Касперского" информацию об использовании KSN, а также может отправлять другую информацию в зависимости от выбранного вами режима использования KSN (*стандартный KSN* или *расширенный KSN*). Режим KSN влияет на объем данных, которые передаются в "Лабораторию Касперского" при использовании KSN.
- Локальный KSN – инфраструктура расположена внутри корпоративной сети организации или на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера.

Информацию о том, какой тип и режим KSN использует программа Kaspersky Security, вы может получить у провайдера антивирусной защиты. Параметры использования KSN определяются политикой провайдера.

> Использование Глобального KSN независимо от выбранного режима использования KSN (стандартный KSN или расширенный KSN) приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN или отказаться от использования KSN.

Участие в Kaspersky Security Network является добровольным. Решение об участии в Kaspersky Security Network принимается при создании политики, его можно изменить в любой момент.

► *Чтобы включить или выключить использование KSN в работе программы Kaspersky Security, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры защиты вашей виртуальной инфраструктуры:
   a. В дереве консоли выберите папку **Управляемые устройства**.
   b. В рабочей области выберите закладку **Политики**.
   c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
2. В окне свойств политики выберите раздел **Параметры KSN**.
3. Если вы хотите включить использование KSN в работе программы, выполните следующие действия:
   a. Установите флажок **Использовать KSN**.
   b. В открывшемся окне ознакомьтесь с Положением о Kaspersky Security Network.
   c. Если вы согласны со всеми пунктами Положения, выберите вариант **Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network** и нажмите на кнопку **ОК**.
4. Если вы хотите выключить использование KSN, снимите флажок **Использовать KSN**.
5. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

KSN используется в работе Kaspersky Security, только если провайдер антивирусной защиты включил использование KSN.

Получение информации о состоянии защиты

Программа Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center служебные сообщения с информацией о работе программы – *события*. Информация о событиях сохраняется в базе данных Сервера администрирования.

Выделяют следующие уровни важности событий:

- **Критическое событие**. Событие критической важности, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке. Может указывать на проблемы в работе Kaspersky Security или на уязвимости в защите виртуальных машин.
- **Отказ функционирования**. Событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- **Предупреждение**. Событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky Security и может указывать на возможную проблему в будущем.
- **Информационное сообщение**. Событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

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". На закладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл. Подробнее о работе с выборками событий см. в документации Kaspersky Security Center.

Уведомление – это сообщение с информацией о событии. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе программы. Для выбора способа уведомления о событиях и настройки других параметров уведомлений о событиях вам нужно обратиться к провайдеру антивирусной защиты.

Подробную информацию о событиях и уведомлениях см. в документации Kaspersky Security Center.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать срочные пакеты обновлений программного обеспечения, устраняющие уязвимости и ошибки. Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского".

Для сохранения бинарной целостности сертифицированной программы запрещается устанавливать обновления программных модулей, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления программных модулей необходимо получать путем обращения в техническую поддержку АО "Лаборатория Касперского" по телефонам: +7 (495) 663-81-47, 8-800-700-88-11 или из регулярно обновляемых статей об актуальных версиях сертифицированных программ на сайте разработчика-изготовителя (http://support.kaspersky.ru/general/certificates). Информацию об обновлениях следует проверять не реже, чем один раз в месяц.

Программы должны периодически (один раз в полгода) подвергаться анализу уязвимостей: компания, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с сайта разработчика-изготовителя (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках 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" (https://community.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 173).

kaspersky

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 вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону (http://support.kaspersky.ru/b2b).
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

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" (http://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Red Hat Enterprise Linux – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак компании Red Hat, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

VMware, VMware ESXi, Mware NSX Manager, VMware NSX for vSphere, VMware vCenter Server, VMware vCloud Director, VMware Tools, VMware vSphere и VMware vSphere Web Client – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

kaspersky

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 2. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура	среда функционирования
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

kaspersky

Приложение. Значения параметров программы в сертифицированном состоянии

Этот раздел содержит перечень параметров программы, влияющих на сертифицированное состояние программы, и значений параметров в сертифицированном состоянии.

Если вы меняете какие-либо из перечисленных параметров с их значений в сертифицированном состоянии на другие значения, вы выводите программу из сертифицированного состояния.

Таблица 3. Параметры и их значения для программы в сертифицированном состоянии

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Защищаемая инфраструктура в политике	**Использовать защиту от файловых угроз**	Флажок установлен.
Защищаемая инфраструктура в политике	**Профиль защиты**	Одно из следующих значений: • **унаследованный: <N>**, где N – имя унаследованного от родительского объекта профиля защиты; • **<N>**, где N – название назначенного профиля защиты, в том числе **Основной профиль защиты**.
Основной профиль защиты, дополнительный профиль защиты	**Действие при обнаружении угрозы**	Одно из следующих значений: • **Лечить. Блокировать, если лечение невозможно**. • **Лечить. Удалять, если лечение невозможно**. • **Удалять. Блокировать, если удаление невозможно**. • **Блокировать**.
Задача полной проверки, задача выборочной проверки	**Действие при обнаружении угрозы** в блоке **Проверка включенных виртуальных машин**	Одно из следующих значений: • **Лечить. Блокировать, если лечение невозможно**. • **Лечить. Удалять, если лечение невозможно**. • **Удалять. Блокировать, если удаление невозможно**. • **Блокировать**.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Основной профиль защиты, дополнительный профиль защиты	**Проверять сетевые диски** в блоке **Область защиты**	Флажок установлен при наличии сетевых дисков на защищаемой виртуальной машине. Если сетевые диски отсутствуют, флажок может быть снят.
Задача полной проверки, задача выборочной проверки	**Проверять оптические диски** в блоке **Проверка включенных виртуальных машин**	Флажок установлен при наличии оптического привода на защищаемой виртуальной машине. Если оптический привод отсутствует, флажок может быть снят.
Основной профиль защиты, дополнительный профиль защиты, задача полной проверки, задача выборочной проверки	**Проверять все, кроме файлов со следующими расширениями**	Пусто.
Основной профиль защиты, дополнительный профиль защиты, задача полной проверки, задача выборочной проверки	**Проверять только файлы со следующими расширениями**	Пусто.
Основной профиль защиты	**Папки и файлы**	Пусто или только заданный по умолчанию список исключений, рекомендуемых корпорацией Microsoft.
Дополнительный профиль защиты, задача полной проверки, задача выборочной проверки	**Папки и файлы**	Пусто.
Параметры использования KSN в свойствах политики	**Использовать KSN**	Флажок снят.
Параметры использования KSN в свойствах политики	**Использовать расширенный KSN**	Флажок снят.
Параметры использования KSN в мастере создания политики	**Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network**	Вариант не выбран.
Параметры использования KSN в мастере создания политики	**Я не принимаю условия настоящего Положения о Kaspersky Security Network**	Вариант выбран.
Параметры резервного хранилища в политике	**Помещать файлы в резервное хранилище**	Флажок установлен.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Параметры событий Kaspersky Security в политике	**На Сервере администрирования в течение (сут)**	Флажок установлен, значение не ниже заданного по умолчанию.
Задача обновления баз программы	**Запуск по расписанию**	**При загрузке обновлений в хранилище**.