KASPERSKY

Kaspersky Security для виртуальных сред 4.0 Защита без агента

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 4.1.0.47

Уважаемый пользователь!

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

Дата редакции документа: 07.06.2017

Обозначение документа: 643.46856491.00098-01 90 01

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

Содержание

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Security для виртуальных сред 4.0 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.

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;
- форум "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. 186).

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 (http://support.kaspersky.ru/ksv4nola) 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.

Форум

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (http://forum.kaspersky.com).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

О программе

Программное изделие "Kaspersky Security для виртуальных сред 4.0 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.

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 10 Service Pack 2 Maintenance Release 1.
- Kaspersky Security Center 10 Service Pack 2.

> Полная функциональность программы Kaspersky Security для виртуальных сред 4.0 Защита без агента доступна только при использовании Kaspersky Security Center версии Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

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® 2016 (64-разрядная).
- Windows Server 2012 R2 Datacenter / Standard (64-разрядная).
- Windows Server 2012 R2 Essentials (64-разрядная).
- Windows Server 2012 Datacenter / Standard (64-разрядная).
- Windows Server 2012 Essentials (64-разрядная).
- Windows Server 2008 R2 Datacenter / Enterprise / Standard Service Pack 1 (64-разрядная).
- Windows Server 2008 Datacenter / Enterprise / Standard Service Pack 2 (32 / 64-разрядная).

Для установки Сервера интеграции, Консоли управления Сервера интеграции и плагина управления Kaspersky Security требуется платформа Microsoft® .NET Framework 4.6.

Программные требования компонента Файловый Антивирус в виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager версии 6.3.1

Если вы используете платформу VMware NSX™ for vSphere™ версии 6.3.1, для функционирования компонента Файловый Антивирус виртуальная инфраструктура должна удовлетворять следующим программным требованиям:

- Гипервизор VMware ESXi™ 6.5a, гипервизор VMware ESXi 6.0 исправление 3 или гипервизор VMware ESXi 5.5 исправление 3b.

- Пакет VMware Tools™ одной из следующих версий:
  - 10.0.12 (сборка 4448496), если на виртуальной машине установлена операционная система Windows Server 2003 R2.
  - 10.1.0 (сборка 4449150) или 10.1.5 (сборка 5055683), если на виртуальной машине установлена другая поддерживаемая операционная система Windows®.

  При установке пакета VMware Tools должен быть установлен компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver. При установке пакета VMware Tools с параметрами по умолчанию компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver не будет установлен.

  > Информацию об обновлении VMware Tools см. в документации к продуктам VMware™.

- Сервер VMware vCenter™ 6.5a, сервер VMware vCenter 6.0 исправление 3 или сервер VMware vCenter 5.5 исправление 3e.
- VMware NSX for vSphere 6.3.1.
- Для защиты виртуальных машин с операционной системой Linux®: драйвер VMware Linux Thin Agent (vmware-nsx-gi-file-1.0.0.4888131).

  > Сведения об установке драйвера VMware Linux Thin Agent см. в документации к VMware NSX for vSphere 6.3.

В виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager™ версии 6.3.1 компонент Файловый Антивирус обеспечивает защиту виртуальных машин, на которых установлены следующие гостевые операционные системы:

- Настольные операционные системы Windows:
  - Windows 10 (32 / 64-разрядная).
  - Windows 8.1 (32 / 64-разрядная).
  - Windows 8 (32 / 64-разрядная).

- Windows 7 Service Pack 1 (32 / 64-разрядная).

- Серверные операционные системы Windows:

  - Windows Server 2012 R2 без поддержки ReFS (Resilient File System) (64-разрядная).

  - Windows Server 2012 без поддержки ReFS (Resilient File System) (64-разрядная).

  - Windows Server 2008 R2 Service Pack 1 (64-разрядная).

  - Windows Server 2003 R2 Service Pack 2 (32 / 64-разрядная).

- Серверные операционные системы Linux:

  - Ubuntu Server 14.04 LTS (64-разрядная).

  - Red Hat Enterprise Linux® Server 7 (64-разрядная).

  - SUSE Linux Enterprise Server 12 (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, nfs4, cifs.

Программные требования компонента Файловый Антивирус в виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager версии 6.2.6

Если вы используете платформу VMware NSX for vSphere 6.2.6, для функционирования компонента Файловый Антивирус виртуальная инфраструктура должна удовлетворять следующим программным требованиям:

- Гипервизор VMware ESXi 6.0 исправление 3 или гипервизор VMware ESXi 5.5 исправление 3b.

- Пакет VMware Tools одной из следующих версий:

- 10.0.12 (сборка 4448496), если на виртуальной машине установлена операционная система Windows Server 2003 R2.
- 10.1.0 (сборка 4449150) или 10.1.5 (сборка 5055683), если на виртуальной машине установлена другая поддерживаемая операционная система Windows.

При установке пакета VMware Tools должен быть установлен компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver. При установке пакета VMware Tools с параметрами по умолчанию компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver не будет установлен.

> Информацию об обновлении VMware Tools см. в документации к продуктам VMware.

- Сервер VMware vCenter 6.0 исправление 3 или сервер VMware vCenter 5.5 исправление 3e.
- VMware NSX for vSphere 6.2.6.

В виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager версии 6.2.6 компонент Файловый Антивирус обеспечивает защиту виртуальных машин, на которых установлены следующие гостевые операционные системы:

- Настольные операционные системы:
  - Windows 10 (32 / 64-разрядная).
  - Windows 8.1 (32 / 64-разрядная).
  - Windows 8 (32 / 64-разрядная).
  - Windows 7 Service Pack 1 (32 / 64-разрядная).
- Серверные операционные системы:
  - Windows Server 2012 R2 без поддержки ReFS (Resilient File System) (64-разрядная).
  - Windows Server 2012 без поддержки ReFS (Resilient File System) (64-разрядная).

- Windows Server 2008 R2 Service Pack 1 (64-разрядная).
- Windows Server 2003 R2 Service Pack 2 (32 / 64-разрядная).

Программные требования компонента Файловый Антивирус в виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager

Техническая поддержка пользователей, использующих инфраструктуру под управлением сервера VMware vCenter и VMware vShield Manager, осуществляется только в рамках расширенной технической поддержки (Kaspersky Maintenance Service Agreement, Enterprise / Business / Plus). Техническая поддержка пользователей, использующих инфраструктуру под управлением сервера VMware vCenter и VMware NSX Manager, осуществляется в рамках стандартной технической поддержки.

Для функционирования компонента Файловый Антивирус виртуальная инфраструктура под управлением сервера VMware vCenter и VMware vShield Manager должна удовлетворять следующим программным требованиям:

- Гипервизор VMware ESXi 6.0 исправление 2 или гипервизор VMware ESXi 5.5 исправление 3b.
- Пакет VMware Tools одной из следующих версий:
  - 10.0.12 (сборка 4448496), если на виртуальной машине установлена операционная система Windows XP или Windows Server 2003 R2.
  - 10.1.0 (сборка 4449150) или 10.1.5 (сборка 5055683), если на виртуальной машине установлена другая поддерживаемая операционная система Windows.

  При установке пакета VMware Tools должен быть установлен компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver. При установке пакета VMware Tools с параметрами по умолчанию компонент VMware Device Drivers / VMCI Driver / NSX File Introspection Driver не будет установлен.

  Информацию об обновлении VMware Tools см. в документации к продуктам VMware.

- Сервер VMware vCenter 6.0 исправление 2 или сервер VMware vCenter 5.5 исправление 3e.
- VMware vShield Endpoint™ из пакета VMware vCloud™ Networking and Security 5.5.4.3.
- VMware vShield Manager™ из пакета VMware vCloud Networking and Security 5.5.4.3.

В виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager компонент Файловый Антивирус обеспечивает защиту виртуальных машин, на которых установлены следующие гостевые операционные системы:

- Настольные операционные системы:
  - Windows 10 (32 / 64-разрядная).
  - Windows 8.1 (32 / 64-разрядная).
  - Windows 8 (32 / 64-разрядная).
  - Windows 7 Service Pack 1 (32 / 64-разрядная).
  - Windows XP SP3 (32-разрядная).
- Серверные операционные системы:
  - Windows Server 2012 R2 без поддержки ReFS (Resilient File System) (64-разрядная).
  - Windows Server 2012 без поддержки ReFS (Resilient File System) (64-разрядная).
  - Windows Server 2008 R2 Service Pack 1 (64-разрядная).
  - Windows Server 2003 R2 Service Pack 2 (32 / 64-разрядная).

Аппаратные требования

Для SVM (виртуальная машина защиты) с установленным компонентом Файловый Антивирус требуется выделить следующее минимальное количество системных ресурсов:

- объем выделенной оперативной памяти – 2 ГБ;
- количество процессоров – 2;

- объем выделенного свободного места на диске – 30 ГБ.

> Если не настроена запись подробной информации в журналы Kaspersky Security, для работы программы требуется 7 ГБ свободного места на диске. Запись подробной информации необходима для диагностики работы программы. Информацию о том, как настроить запись подробной информации в журналы Kaspersky Security, вы можете получить у специалистов Службы технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 186).

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

- объем свободного места на диске – 500 МБ;
- объем оперативной памяти:
  - для работы Консоли управления 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 попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.

16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

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. 11).
- Подготовить образ SVM с компонентом Файловый Антивирус (см. раздел "Подготовка образа SVM" на стр. 28).
- Если вы используете инфраструктуру под управлением сервера VMware vCenter и VMware NSX Manager, разместить все файлы образа SVM в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS.
- Подготовить виртуальную инфраструктуру VMware к установке программы (см. раздел "Подготовка виртуальной инфраструктуры VMware" на стр. 22).
- 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. 27).
- Настроить параметры учетных записей сервера VMware vCenter и VMware NSX Manager, которые требуются для установки и работы программы (см. раздел "Учетные записи для установки и работы программы" на стр. 25).

В этом разделе

Подготовка виртуальной инфраструктуры VMware

Перед установкой программы в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager требуется выполнить следующие действия:

- Объединить гипервизоры VMware ESXi в один или несколько кластеров VMware.
- На каждом кластере VMware развернуть службу Guest Introspection (см. раздел "Развертывание службы Guest Introspection" на стр. 24).
- Установить на каждой виртуальной машине с операционной системой Windows, которую вы хотите защищать с помощью Kaspersky Security, драйвер VMware NSX File Introspection.

  Драйвер VMware NSX File Introspection входит в комплект VMware Tools. В зависимости от операционной системы виртуальной машины требуется установить драйвер VMware NSX File Introspection из комплекта VMware Tools одной из следующих версий:

  - 10.0.12 (сборка 4448496), если на виртуальной машине установлена операционная система Windows Server 2003.

- 10.1.0 (сборка 4449150) или 10.1.5 (сборка 5055683), если на виртуальной машине установлена другая поддерживаемая операционная система Windows.

Сведения о драйвере VMware NSX File Introspection см. в документации к продуктам VMware.

- Установить на каждой виртуальной машине с операционной системой Linux, которую вы хотите защищать с помощью Kaspersky Security, драйвер VMware Linux Thin Agent.

  Сведения об установке драйвера VMware Linux Thin Agent см. в документации к VMware NSX for vSphere 6.3.

  > Kaspersky Security обеспечивает защиту виртуальных машин с операционными системами Linux, только если вы используете платформу VMware NSX for vSphere версии 6.3.1.

Перед установкой программы в инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager требуется установить на каждой виртуальной машине, которую вы хотите защищать с помощью Kaspersky Security, драйвер VMware NSX File Introspection.

Драйвер VMware NSX File Introspection входит в комплект VMware Tools. В зависимости от гостевой операционной системы виртуальной машины требуется установить драйвер VMware NSX File Introspection из комплекта VMware Tools одной из следующих версий:

- 10.0.12 (сборка 4448496), если на виртуальной машине установлена операционная система Windows XP или Windows Server 2003.
- 10.1.0 (сборка 4449150) или 10.1.5 (сборка 5055683), если на виртуальной машине установлена другая поддерживаемая операционная система Windows.

Сведения о драйвере VMware NSX File Introspection см. в документации к продуктам VMware.

Развертывание службы Guest Introspection

Для функционирования Kaspersky Security в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager требуется развернуть службу Guest Introspection на каждом кластере VMware, виртуальные машины которого вы хотите защищать.

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**, 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 программу Kaspersky Security.

   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/13172.

Учетные записи для установки и работы программы

Для установки плагина управления Kaspersky Security и Сервера интеграции требуется учетная запись, которая входит в группу локальных администраторов на компьютере, где выполняется установка.

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

Для установки и удаления программы в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager требуется учетная запись NSX Manager, которой назначена роль Enterprise Administrator.

Для установки и удаления программы в инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager требуется учетная запись администратора сервера VMware vCenter, которой назначена системная роль со следующими правами:

- Global.Licenses
- Datastore.Allocate space
- vApp.Import
- Network.Assign network
- Host.Inventory.Modify cluster

- Host.Configuration.Virtual machine autostart configuration
- Tasks.Create task
- Global.Cancel task
- Virtual machine.Configuration.Add new disk
- Virtual machine.Interaction.Power On
- Virtual machine.Inventory.Create new
- Virtual machine.Interaction.Power Off
- Virtual machine.Inventory.Remove
- Virtual machine.Interact.Device connection

Имя и пароль учетной записи администратора не сохраняются в параметрах программы.

Независимо от используемой инфраструктуры для работы программы и изменения конфигурации SVM требуется учетная запись сервера VMware vCenter, которой назначена предустановленная системная роль ReadOnly. Системная роль ReadOnly по умолчанию имеет права System.View, System.Read и System.Anonymous. Для обеспечения возможности проверки выключенных виртуальных машин необходимо назначить этой учетной записи следующие права:

- Virtual machine.Configuration.Add existing disk
- Virtual machine.Configuration.Remove disk
- Virtual machine.Configuration.Add or remove device

Имя и пароль учетной записи хранятся на Сервере интеграции в защищенном виде.

> Роли должны быть назначены учетным записям на верхнем уровне иерархии объектов управления VMware – на уровне сервера VMware vCenter.

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

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.
443 TCP	От Сервера интеграции к VMware vShield Manager или VMware NSX Manager.	Для взаимодействия Сервера интеграции с виртуальной инфраструктурой.
443 TCP	От Сервера интеграции к серверу VMware vCenter.	Для взаимодействия Сервера интеграции с виртуальной инфраструктурой.

Подготовка образа SVM

Программа Kaspersky Security поставляется в виде бинарных компонентов. Перед началом установки программы необходимо создать образ SVM с установленным компонентом Файловый Антивирус.

► *Чтобы создать образ SVM с установленным компонентом Файловый Антивирус, выполните следующие действия:*

1. Создайте виртуальную машину с установленной операционной системой CentOS 6.8.
2. Войдите в систему на созданной виртуальной машине под учетной записью root.
3. Установите VMware ovftool 3.0.1 (дистрибутив доступен по адресу https://www.vmware.com/support/developer/ovf).
4. Установите из CentOS-репозитория утилиты kpartx и qemu-img:

   ```
   yum install kpartx qemu-img
   ```

5. Скопируйте сборочные скрипты и необходимые библиотеки (все содержимое папки centos_build4.1) в локальную папку /root/centos_build4.1.
6. Скопируйте в папку /root/centos_build4.1/centos_rpms файл centos-release-6-8.el6.centos.12.3.x86_64.rpm.
7. Скопируйте в папку /root/centos_build4.1/centos_rpms_4.1.0-47g пакеты из списка 1 (см. ниже).
8. Скопируйте в папку /root/centos_build4.1/vmware_rpms пакеты из списка 2 (см. ниже).
9. Скопируйте в папку /root/centos_build4.1/ksv_rpms пакеты из списка 3 (см. ниже).
10. Распакуйте в папку /root/centos_build4.1/ архив patch4.1.0.47g.tar.bz2.
11. Перейдите в сборочную папку.
12. Выполните команду:

    ```
    bash /img.sh -p ksv -v 4.1.0-47g -f centos_rpms_4.1.0-47g -k 0 -m 0 -patch-folder patch4.1.0.47g -certification
    ```

Результат сборки появится в /root/centos_build4.1/build_iso/ksv-4.1.0-47g.x86_64.el6.*

Список 1

1. acl-2.2.49-6.el6.x86_64.rpm
2. attr-2.4.44-7.el6.x86_64.rpm
3. audit-2.4.5-3.el6.x86_64.rpm
4. audit-libs-2.4.5-3.el6.x86_64.rpm
5. authconfig-6.1.12-23.el6.x86_64.rpm
6. basesystem-10.0-4.el6.noarch.rpm
7. bash-4.1.2-41.el6_8.x86_64.rpm
8. bc-1.06.95-1.el6.x86_64.rpm
9. binutils-2.20.51.0.2-5.44.el6.x86_64.rpm
10. bzip2-1.0.5-7.el6_0.x86_64.rpm
11. bzip2-libs-1.0.5-7.el6_0.x86_64.rpm
12. ca-certificates-2015.2.6-65.0.1.el6_7.noarch.rpm
13. checkpolicy-2.0.22-1.el6.x86_64.rpm
14. chkconfig-1.3.49.5-1.el6.x86_64.rpm
15. coreutils-8.4-43.el6.x86_64.rpm
16. coreutils-libs-8.4-43.el6.x86_64.rpm
17. cpio-2.10-12.el6_5.x86_64.rpm
18. cracklib-2.8.16-4.el6.x86_64.rpm
19. cracklib-dicts-2.8.16-4.el6.x86_64.rpm
20. cronie-1.4.4-16.el6_8.2.x86_64.rpm
21. cronie-anacron-1.4.4-16.el6_8.2.x86_64.rpm
22. crontabs-1.10-33.el6.noarch.rpm

23. cryptsetup-luks-1.2.0-11.el6.x86_64.rpm
24. cryptsetup-luks-libs-1.2.0-11.el6.x86_64.rpm
25. curl-7.19.7-52.el6.x86_64.rpm
26. cyrus-sasl-2.1.23-15.el6_6.2.x86_64.rpm
27. cyrus-sasl-lib-2.1.23-15.el6_6.2.x86_64.rpm
28. dash-0.5.5.1-4.el6.x86_64.rpm
29. db4-4.7.25-20.el6_8.1.x86_64.rpm
30. db4-utils-4.7.25-20.el6_8.1.x86_64.rpm
31. dbus-glib-0.86-6.el6.x86_64.rpm
32. dbus-libs-1.2.24-8.el6_6.x86_64.rpm
33. device-mapper-1.02.117-7.el6_8.1.x86_64.rpm
34. device-mapper-event-1.02.117-7.el6_8.1.x86_64.rpm
35. device-mapper-event-libs-1.02.117-7.el6_8.1.x86_64.rpm
36. device-mapper-libs-1.02.117-7.el6_8.1.x86_64.rpm
37. device-mapper-multipath-0.4.9-93.el6.x86_64.rpm
38. device-mapper-multipath-libs-0.4.9-93.el6.x86_64.rpm
39. device-mapper-persistent-data-0.6.2-0.1.rc7.el6.x86_64.rpm
40. dhclient-4.1.1-51.P1.el6.centos.x86_64.rpm
41. dhcp-4.1.1-51.P1.el6.centos.x86_64.rpm
42. dhcp-common-4.1.1-51.P1.el6.centos.x86_64.rpm
43. dialog-1.1-9.20080819.1.el6.x86_64.rpm
44. diffutils-2.8.1-28.el6.x86_64.rpm
45. dmidecode-2.12-7.el6.x86_64.rpm
46. dracut-004-409.el6_8.2.noarch.rpm

47. dracut-kernel-004-409.el6_8.2.noarch.rpm
48. e2fsprogs-1.41.12-22.el6.x86_64.rpm
49. e2fsprogs-libs-1.41.12-22.el6.x86_64.rpm
50. elfutils-libelf-0.164-2.el6.x86_64.rpm
51. ethtool-3.5-6.el6.x86_64.rpm
52. expat-2.0.1-13.el6_8.x86_64.rpm
53. file-5.04-30.el6.x86_64.rpm
54. file-libs-5.04-30.el6.x86_64.rpm
55. filesystem-2.4.30-3.el6.x86_64.rpm
56. findutils-4.4.2-9.el6.x86_64.rpm
57. fipscheck-1.2.0-7.el6.x86_64.rpm
58. fipscheck-lib-1.2.0-7.el6.x86_64.rpm
59. fuse-2.8.3-5.el6.x86_64.rpm
60. gamin-0.1.10-9.el6.x86_64.rpm
61. gawk-3.1.7-10.el6_7.3.x86_64.rpm
62. gdb-7.2-90.el6.x86_64.rpm
63. gdbm-1.8.0-39.el6.x86_64.rpm
64. glib2-2.28.8-5.el6.x86_64.rpm
65. glibc-2.12-1.192.el6.i686.rpm
66. glibc-2.12-1.192.el6.x86_64.rpm
67. glibc-common-2.12-1.192.el6.x86_64.rpm
68. gmp-4.3.1-10.el6.x86_64.rpm
69. gnupg2-2.0.14-8.el6.x86_64.rpm
70. gpgme-1.1.8-3.el6.x86_64.rpm

71. gpm-libs-1.20.6-12.el6.x86_64.rpm
72. grep-2.20-5.el6_8.x86_64.rpm
73. groff-1.18.1.4-21.el6.x86_64.rpm
74. grub-0.97-94.el6_7.1.x86_64.rpm
75. grubby-7.0.15-7.el6.x86_64.rpm
76. gzip-1.3.12-22.el6.x86_64.rpm
77. hwdata-0.233-16.1.el6.noarch.rpm
78. info-4.13a-8.el6.x86_64.rpm
79. initscripts-9.03.53-1.el6.centos.2.x86_64.rpm
80. iproute-2.6.32-54.el6.x86_64.rpm
81. iptables-1.4.7-16.el6.x86_64.rpm
82. iptables-ipv6-1.4.7-16.el6.x86_64.rpm
83. iputils-20071127-21.el6.x86_64.rpm
84. iscsi-initiator-utils-6.2.0.873-22.el6_8.x86_64.rpm
85. kbd-1.15-11.el6.x86_64.rpm
86. kbd-misc-1.15-11.el6.noarch.rpm
87. kernel-2.6.32-642.15.1.el6.x86_64.rpm
88. kernel-firmware-2.6.32-642.15.1.el6.noarch.rpm
89. keyutils-libs-1.4-5.el6.x86_64.rpm
90. kpartx-0.4.9-93.el6.x86_64.rpm
91. krb5-libs-1.10.3-57.el6.x86_64.rpm
92. less-436-13.el6.x86_64.rpm
93. libacl-2.2.49-6.el6.x86_64.rpm
94. libaio-0.3.107-10.el6.x86_64.rpm

95. libattr-2.4.44-7.el6.x86_64.rpm
96. libblkid-2.17.2-12.24.el6_8.3.x86_64.rpm
97. libcap-2.16-5.5.el6.x86_64.rpm
98. libcap-ng-0.6.4-3.el6_0.1.x86_64.rpm
99. libcom_err-1.41.12-22.el6.x86_64.rpm
100. libcurl-7.19.7-52.el6.x86_64.rpm
101. libdrm-2.4.65-2.el6.x86_64.rpm
102. libedit-2.11-4.20080712cvs.1.el6.x86_64.rpm
103. libevent-1.4.13-4.el6.x86_64.rpm
104. libffi-3.0.5-3.2.el6.x86_64.rpm
105. libgcc-4.4.7-17.el6.i686.rpm
106. libgcc-4.4.7-17.el6.x86_64.rpm
107. libgcrypt-1.4.5-12.el6_8.x86_64.rpm
108. libgpg-error-1.7-4.el6.x86_64.rpm
109. libidn-1.18-2.el6.x86_64.rpm
110. libnih-1.0.1-7.el6.x86_64.rpm
111. libpcap-1.4.0-4.20130826git2dbcaa1.el6.x86_64.rpm
112. libpciaccess-0.13.4-1.el6.x86_64.rpm
113. libselinux-2.0.94-7.el6.x86_64.rpm
114. libselinux-utils-2.0.94-7.el6.x86_64.rpm
115. libsemanage-2.0.43-5.1.el6.x86_64.rpm
116. libsepol-2.0.41-4.el6.x86_64.rpm
117. libss-1.41.12-22.el6.x86_64.rpm
118. libssh2-1.4.2-2.el6_7.1.x86_64.rpm

119. libstdc++-4.4.7-17.el6.i686.rpm
120. libstdc++-4.4.7-17.el6.x86_64.rpm
121. libtasn1-2.3-6.el6_5.x86_64.rpm
122. libudev-147-2.73.el6_8.2.x86_64.rpm
123. libusb-0.1.12-23.el6.x86_64.rpm
124. libusb1-1.0.9-0.7.rc1.el6.x86_64.rpm
125. libuser-0.56.13-8.el6_7.x86_64.rpm
126. libutempter-1.1.5-4.1.el6.x86_64.rpm
127. libuuid-2.17.2-12.24.el6_8.3.x86_64.rpm
128. libxml2-2.7.6-21.el6_8.1.x86_64.rpm
129. libxml2-python-2.7.6-21.el6_8.1.x86_64.rpm
130. libxslt-1.1.26-2.el6_3.1.x86_64.rpm
131. lm_sensors-libs-3.1.1-17.el6.x86_64.rpm
132. logrotate-3.7.8-26.el6_7.x86_64.rpm
133. lsof-4.82-5.el6.x86_64.rpm
134. lua-5.1.4-4.1.el6.x86_64.rpm
135. lvm2-2.02.143-7.el6_8.1.x86_64.rpm
136. lvm2-libs-2.02.143-7.el6_8.1.x86_64.rpm
137. m4-1.4.13-5.el6.x86_64.rpm
138. make-3.81-23.el6.x86_64.rpm
139. MAKEDEV-3.24-6.el6.x86_64.rpm
140. mc-4.7.0.2-6.el6.x86_64.rpm
141. memcached-1.4.4-3.el6_8.1.x86_64.rpm
142. mingetty-1.08-5.el6.x86_64.rpm

143. module-init-tools-3.9-25.el6.x86_64.rpm
144. mysql-libs-5.1.73-8.el6_8.x86_64.rpm
145. ncurses-5.7-4.20090207.el6.x86_64.rpm
146. ncurses-base-5.7-4.20090207.el6.x86_64.rpm
147. ncurses-libs-5.7-4.20090207.el6.x86_64.rpm
148. net-snmp-5.5-57.el6_8.1.x86_64.rpm
149. net-snmp-libs-5.5-57.el6_8.1.x86_64.rpm
150. net-tools-1.60-110.el6_2.x86_64.rpm
151. newt-0.52.11-3.el6.x86_64.rpm
152. newt-python-0.52.11-3.el6.x86_64.rpm
153. nspr-4.11.0-1.el6.x86_64.rpm
154. nss-3.21.3-2.el6_8.x86_64.rpm
155. nss-softokn-3.14.3-23.3.el6_8.x86_64.rpm
156. nss-softokn-freebl-3.14.3-23.3.el6_8.i686.rpm
157. nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64.rpm
158. nss-sysinit-3.21.3-2.el6_8.x86_64.rpm
159. nss-tools-3.21.3-2.el6_8.x86_64.rpm
160. nss-util-3.21.3-1.el6_8.x86_64.rpm
161. openldap-2.4.40-12.el6.x86_64.rpm
162. openssh-5.3p1-118.1.el6_8.x86_64.rpm
163. openssh-clients-5.3p1-118.1.el6_8.x86_64.rpm
164. openssh-server-5.3p1-118.1.el6_8.x86_64.rpm
165. openssl-1.0.1e-48.el6_8.4.x86_64.rpm
166. p11-kit-0.18.5-2.el6_5.2.x86_64.rpm

167. p11-kit-trust-0.18.5-2.el6_5.2.x86_64.rpm
168. pam-1.1.1-22.el6.x86_64.rpm
169. parted-2.1-29.el6.x86_64.rpm
170. passwd-0.77-7.el6.x86_64.rpm
171. pciutils-3.1.10-4.el6.x86_64.rpm
172. pciutils-libs-3.1.10-4.el6.x86_64.rpm
173. pcre-7.8-7.el6.x86_64.rpm
174. perl-5.10.1-141.el6_7.1.x86_64.rpm
175. perl-libs-5.10.1-141.el6_7.1.x86_64.rpm
176. perl-Module-Pluggable-3.90-141.el6_7.1.x86_64.rpm
177. perl-Pod-Escapes-1.04-141.el6_7.1.x86_64.rpm
178. perl-Pod-Simple-3.13-141.el6_7.1.x86_64.rpm
179. perl-URI-1.40-2.el6.noarch.rpm
180. perl-version-0.77-141.el6_7.1.x86_64.rpm
181. perl-XML-LibXML-1.70-5.el6.x86_64.rpm
182. perl-XML-NamespaceSupport-1.10-3.el6.noarch.rpm
183. perl-XML-SAX-0.96-7.el6.noarch.rpm
184. pinentry-0.7.6-8.el6.x86_64.rpm
185. pkgconfig-0.23-9.1.el6.x86_64.rpm
186. plymouth-0.8.3-27.el6.centos.1.x86_64.rpm
187. plymouth-core-libs-0.8.3-27.el6.centos.1.x86_64.rpm
188. plymouth-scripts-0.8.3-27.el6.centos.1.x86_64.rpm
189. policycoreutils-2.0.83-30.1.el6_8.x86_64.rpm
190. popt-1.13-7.el6.x86_64.rpm

191. portreserve-0.0.4-11.el6.x86_64.rpm
192. postfix-2.6.6-6.el6_7.1.x86_64.rpm
193. procps-3.2.8-36.el6.x86_64.rpm
194. psmisc-22.6-19.el6_5.x86_64.rpm
195. pth-2.0.7-9.3.el6.x86_64.rpm
196. pygpgme-0.1-18.20090824bzr68.el6.x86_64.rpm
197. python-2.6.6-66.el6_8.x86_64.rpm
198. python-iniparse-0.3.1-2.1.el6.noarch.rpm
199. python-libs-2.6.6-66.el6_8.x86_64.rpm
200. python-lxml-2.2.3-1.1.el6.x86_64.rpm
201. python-pycurl-7.19.0-9.el6.x86_64.rpm
202. python-urlgrabber-3.9.1-11.el6.noarch.rpm
203. readline-6.0-4.el6.x86_64.rpm
204. redhat-logos-60.0.14-12.el6.centos.noarch.rpm
205. rootfiles-8.1-6.1.el6.noarch.rpm
206. rpm-4.8.0-55.el6.x86_64.rpm
207. rpm-libs-4.8.0-55.el6.x86_64.rpm
208. rpm-python-4.8.0-55.el6.x86_64.rpm
209. rsyslog-5.8.10-10.el6_6.x86_64.rpm
210. sed-4.2.1-10.el6.x86_64.rpm
211. setup-2.8.14-20.el6_4.1.noarch.rpm
212. shadow-utils-4.1.5.1-5.el6.x86_64.rpm
213. shared-mime-info-0.70-6.el6.x86_64.rpm
214. slang-2.2.1-1.el6.x86_64.rpm

215. source_rpms.list
216. sqlite-3.6.20-1.el6_7.2.x86_64.rpm
217. strace-4.8-10.el6.x86_64.rpm
218. sudo-1.8.6p3-25.el6_8.x86_64.rpm
219. system-config-firewall-base-1.2.27-7.2.el6_6.noarch.rpm
220. sysvinit-tools-2.87-6.dsf.el6.x86_64.rpm
221. tar-1.23-15.el6_8.x86_64.rpm
222. tcpdump-4.0.0-9.20090921gitdf3cb4.2.el6.x86_64.rpm
223. tcp_wrappers-libs-7.6-58.el6.x86_64.rpm
224. tzdata-2016j-1.el6.noarch.rpm
225. udev-147-2.73.el6_8.2.x86_64.rpm
226. unzip-6.0-4.el6.x86_64.rpm
227. upstart-0.6.5-16.el6.x86_64.rpm
228. ustr-1.0.4-9.1.el6.x86_64.rpm
229. util-linux-ng-2.17.2-12.24.el6_8.3.x86_64.rpm
230. vim-common-7.4.629-5.el6_8.1.x86_64.rpm
231. vim-enhanced-7.4.629-5.el6_8.1.x86_64.rpm
232. vim-filesystem-7.4.629-5.el6_8.1.x86_64.rpm
233. vim-minimal-7.4.629-5.el6_8.1.x86_64.rpm
234. wget-1.12-8.el6.x86_64.rpm
235. which-2.19-6.el6.x86_64.rpm
236. xz-libs-4.999.9-0.5.beta.20091007git.el6.x86_64.rpm
237. yum-3.2.29-75.el6.centos.noarch.rpm
238. yum-metadata-parser-1.1.2-16.el6.x86_64.rpm

239. yum-plugin-fastestmirror-1.1.30-37.el6.noarch.rpm

240. yum-utils-1.1.30-37.el6.noarch.rpm

241. zlib-1.2.3-29.el6.x86_64.rpm

Список 2

1. kmod-vmware-tools-pvscsi-1.2.3.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
2. kmod-vmware-tools-vmci-9.8.1.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
3. kmod-vmware-tools-vmhgfs-2.0.17.1-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
4. kmod-vmware-tools-vmmemctl-1.3.2.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
5. kmod-vmware-tools-vmxnet-2.1.0.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
6. kmod-vmware-tools-vmxnet3-1.4.2.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
7. kmod-vmware-tools-vsock-9.8.1.0-2.6.32.71.el6.x86_64.5.el6.x86_64.rpm
8. ksv-tools-1.0.0-4.x86_64.rpm
9. vmware-studio-vami-tools_2.5.0.0-387333_x86_64.rpm
10. vmware-tools-core-10.0.9-1.el6.x86_64.rpm
11. vmware-tools-esx-nox-10.0.9-1.el6.x86_64.rpm
12. vmware-tools-foundation-10.0.9-1.el6.x86_64.rpm
13. vmware-tools-guestlib-10.0.9-1.el6.x86_64.rpm
14. vmware-tools-libraries-nox-10.0.9-1.el6.x86_64.rpm
15. vmware-tools-plugins-autoUpgrade-10.0.9-1.el6.x86_64.rpm
16. vmware-tools-plugins-deployPkg-10.0.9-1.el6.x86_64.rpm
17. vmware-tools-plugins-grabbitmqProxy-10.0.9-1.el6.x86_64.rpm
18. vmware-tools-plugins-guestInfo-10.0.9-1.el6.x86_64.rpm
19. vmware-tools-plugins-hgfsServer-10.0.9-1.el6.x86_64.rpm
20. vmware-tools-plugins-powerOps-10.0.9-1.el6.x86_64.rpm

21. vmware-tools-plugins-timeSync-10.0.9-1.el6.x86_64.rpm
22. vmware-tools-plugins-vix-10.0.9-1.el6.x86_64.rpm
23. vmware-tools-plugins-vmbackup-10.0.9-1.el6.x86_64.rpm
24. vmware-tools-pvscsi-common-10.0.9-5.el6.x86_64.rpm
25. vmware-tools-services-10.0.9-1.el6.x86_64.rpm
26. vmware-tools-vgauth-10.0.9-1.el6.x86_64.rpm
27. vmware-tools-vmblock-common-10.0.9-5.el6.x86_64.rpm
28. vmware-tools-vmci-common-10.0.9-5.el6.x86_64.rpm
29. vmware-tools-vmhgfs-common-10.0.9-5.el6.x86_64.rpm
30. vmware-tools-vmmemctl-common-10.0.9-5.el6.x86_64.rpm
31. vmware-tools-vmxnet3-common-10.0.9-5.el6.x86_64.rpm
32. vmware-tools-vmxnet-common-10.0.9-5.el6.x86_64.rpm
33. vmware-tools-vsock-common-10.0.9-5.el6.x86_64.rpm

Список 3

1. kimul.ko
2. klnagent-10.1.0-93.i386.rpm
3. ksv-4.1.0-47.x86_64.rpm
4. ksv_epsec-4.1.0-47.x86_64.rpm
5. ksv_nsx-4.1.0-47.x86_64.rpm
6. ntfs-3g-2015.3.14-2.el6.x86_64.rpm
7. ova_xml.tar.gz
8. EULA.tar.gz
9. ksv_ksn-4.1.0-47.x86_64.rpm

Установка программы

Порядок установки программы и состав устанавливаемых компонентов зависит от состава инфраструктуры VMware.

Инфраструктура под управлением сервера VMware vCenter и VMware NSX Manager

Установка программы Kaspersky Security в виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager состоит из следующих этапов:

1. Установка плагина управления Kaspersky Security и Сервера интеграции (см. раздел "Установка плагина управления Kaspersky Security и Сервера интеграции" на стр. 43).

2. Настройка параметров подключения Сервера интеграции к одному или нескольким серверам VMware vCenter (см. раздел "Настройка Сервера интеграции" на стр. 45).

3. Развертывание защиты в виртуальной инфраструктуре (см. раздел "Развертывание защиты в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager" на стр. 50):

   a. Регистрация в VMware NSX Manager службы Kaspersky Security: службы защиты файловой системы (Kaspersky File Antimalware Protection).

   b. Настройка группы безопасности NSX (NSX Security Group) и политики безопасности NSX (NSX Security Policy).

   c. Развертывание SVM с компонентом Файловый Антивирус на гипервизорах VMware ESXi. Развертывание SVM выполнятся в результате развертывания службы Kaspersky Security.

   d. Первоначальная настройка конфигурации новых SVM.

4. Подготовка программы к работе (см. раздел "Подготовка программы к работе" на стр. 75):

   - Активация программы на всех новых SVM.

   - Обновление баз программы на всех новых SVM.

- Создание политики, которая будет применяться на SVM.

Инфраструктура под управлением сервера VMware vCenter и VMware vShield Manager

Установка программы Kaspersky Security в виртуальной инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager состоит из следующих этапов:

1. Установка плагина управления Kaspersky Security и Сервера интеграции (см. раздел "Установка плагина управления Kaspersky Security и Сервера интеграции" на стр. 43).

2. Настройка параметров подключения Сервера интеграции к одному или нескольким серверам VMware vCenter (см. раздел "Настройка Сервера интеграции" на стр. 45).

3. Развертывание SVM с компонентом Файловый Антивирус на гипервизорах VMware ESXi (см. раздел "Развертывание защиты в инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager" на стр. 61).

4. Подготовка программы к работе (см. раздел "Подготовка программы к работе" на стр. 75):

   - Активация программы на всех новых SVM.
   - Обновление баз программы на всех новых SVM.
   - Создание политики, которая будет применяться на SVM.

В этом разделе

Установка плагина управления Kaspersky Security и Сервера интеграции

Установку плагина управления Kaspersky Security и компонентов Сервера интеграции следует выполнять под учетной записью, которая входит в группу локальных администраторов.

► *Чтобы установить 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 SecurityCenterComponents_4.1.0.165_setup.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 управления Сервера интеграции.

   Запустится мастер установки.

2. Следуйте указаниям 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 управления Сервера интеграции. Установленный плагин управления Kaspersky Security отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Сервер администрирования**.
3. Откройте окно **Свойства: Сервер администрирования** по ссылке **Свойства** из контекстного меню или по ссылке **Свойства Сервера администрирования** в рабочей области в блоке **Сервер администрирования**.
4. В окне свойств Сервера администрирования в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

   В правой части окна в списке установленных плагинов управления отображается плагин управления Kaspersky Security: **Kaspersky Security для виртуальных сред 4.0 Защита без агента**.

Для взаимодействия Сервера интеграции с Консолью управления, с SVM, с сервером VMware vCenter 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 (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 сертификат Сервера

интеграции утерян или вы хотите использовать более надежный сертификат, вы можете заменить SSL-сертификат Сервера интеграции (процедура замены сертификата описана в Базе знаний http://support.kaspersky.ru/13207).

Настройка Сервера интеграции

После установки Сервера интеграции необходимо выполнить следующие действия:

- Настроить параметры подключения Сервера интеграции к одному или нескольким серверам VMware vCenter (см. раздел "Настройка параметров подключения Сервера интеграции к серверам VMware vCenter" на стр. 48).
- Если вы используете инфраструктуру под управлением сервера VMware vCenter и VMware vShield Manager, изменить пароль учетной записи svm, созданный автоматически во время установки Сервера интеграции (см. раздел "Изменение пароля учетной записи svm" на стр. 47).

Настройка параметров Сервера интеграции выполняется в Консоли управления Сервера интеграции.

В этом разделе

Запуск Консоли управления Сервера интеграции

Если компьютер, на котором установлена Консоль управления Сервера интеграции, входит в домен Microsoft Windows, 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 управления Сервера интеграции, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования**.
3. Запустите Консоль управления Сервера интеграции по ссылке **Запустить Консоль управления Сервера интеграции** в блоке **Развертывание**.
4. Если выполняется одно из следующих условий, откроется окно для ввода параметров подключения к Серверу интеграции:
   - если компьютер, на котором установлена Консоль управления Сервера интеграции, не входит в домен Microsoft Windows;
   - если компьютер, на котором установлена Консоль управления Сервера интеграции, входит в домен, но не удалось подключиться к Серверу интеграции, используя адрес и порт подключения, заданные в параметрах Консоли управления 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 управления 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 управления 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**.

5. Консоль управления 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.

   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 управления Сервера интеграции, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\VIISConsole\Trusted\.

Откроется Консоль управления Сервера интеграции.

Изменение пароля учетной записи svm

Если вы используете инфраструктуру под управлением сервера VMware vCenter и VMware vShield Manager, перед началом развертывания SVM вам требуется изменить пароль учетной записи svm, автоматически созданный во время установки Сервера интеграции. Новый пароль учетной записи svm требуется указать во время развертывания SVM, которые должны подключаться к этому Серверу интеграции.

Если вы используете инфраструктуру под управлением сервера VMware vCenter и VMware NSX Manager, изменять автоматически созданный пароль учетной записи svm не требуется. Сервер интеграции передаст этот пароль на все SVM после их развертывания.

► *Чтобы изменить пароль учетной записи svm, выполните следующие действия:*

1. Запустите Консоль управления Сервера интеграции (см. раздел "Запуск Консоли управления Сервера интеграции" на стр. 46).

2. В разделе **Учетные записи Сервера интеграции** выберите в таблице имя учетной записи svm.

3. По ссылке **Изменить пароль учетной записи** откройте окно **Пароль учетной записи** и введите новый пароль в полях **Пароль** и **Подтверждение пароля**.

   Пароль должен содержать от 1 до 60 символов. Вы можете использовать буквы латинского алфавита, цифры, а также следующие символы: ! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~.

4. Нажмите на кнопку **ОК** в окне **Пароль учетной записи**.

5. Чтобы применить изменения и закрыть Консоль управления, нажмите на кнопку **Закрыть**.

Настройка параметров подключения Сервера интеграции к серверам VMware vCenter

► *Чтобы настроить параметры подключения Сервера интеграции к одному или нескольким серверам VMware vCenter, выполните следующие действия:*

1. Запустите Консоль управления Сервера интеграции (см. раздел "Запуск Консоли управления Сервера интеграции" на стр. 46).

2. Перейдите на закладку **Защита виртуальной инфраструктуры**.

3. Чтобы настроить новое подключение к серверу VMware vCenter, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Параметры подключения** укажите следующие параметры:

      - IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера VMware vCenter, к которому подключается Сервер интеграции;
      - имя и пароль учетной записи, под которой Сервер интеграции подключается к серверу VMware vCenter.

      Введенные параметры подключения к серверу VMware vCenter (кроме пароля) сохраняются в реестре операционной системы в защищенном виде.

   c. Нажмите на кнопку **Добавить**. Окно **Параметры подключения** закроется. Введенный адрес сервера VMware vCenter отображается в таблице. Сервер интеграции проверяет указанные параметры подключения и SSL-сертификат, полученный от сервера VMware vCenter. Если подключиться не удалось или во время подключения обнаружены ошибки сертификата, в таблице отображается предупреждение.

      Если корневой сертификат цепочки сертификатов отсутствует или не является доверенным, вы можете устранить ошибку подключения путем добавления полученного сертификата в список доверенных сертификатов. Для этого по ссылке в описании проблемы откройте окно **Подтверждение сертификата** и нажмите на кнопку **Считать доверенным**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль управления Сервера интеграции.

Если требуется, аналогично укажите параметры подключения к другим серверам VMware vCenter.

В таблице для каждого сервера VMware vCenter отображается список действий, которые вы можете выполнить при настройке подключения к этому серверу VMware vCenter и при развертывании и настройке защиты виртуальной инфраструктуры под управлением этого сервера VMware vCenter. Вы можете развернуть или свернуть список возможных действий

для каждого сервера VMware vCenter щелчком мыши по адресу или имени сервера VMware vCenter в графе **Адрес**.

Если вы хотите изменить параметры подключения к серверу VMware vCenter, разверните список возможных действий для этого сервера VMware vCenter и выберите в списке действие **Изменить параметры подключения к серверу VMware vCenter**. Откроется окно **Параметры подключения**.

Если вы хотите удалить из списка сервер VMware vCenter, разверните список возможных действий для этого сервера VMware vCenter и выберите в списке действие **Удалить сервер VMware vCenter из списка**. Подтвердите удаление в открывшемся окне.

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

Развертывание защиты в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager

Для развертывания защиты в инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager требуется выполнить следующие действия:

1. В Консоли управления Сервера интеграции настроить параметры подключения Сервера интеграции к одному или нескольким серверам VMware vCenter (см. раздел "Настройка параметров подключения Сервера интеграции к серверам VMware vCenter" на стр. 48).

2. Ввести параметры, необходимые для регистрации в VMware NSX Manager и развертывания службы Kaspersky Security: службы защиты файловой системы (Kaspersky File Antimalware Protection). Ввод параметров выполняется в мастере, который запускается из Консоли управления Сервера интеграции (см. раздел "Ввод параметров служб Kaspersky Security" на стр. 52).

По окончании ввода параметров Сервер интеграции выполняет регистрацию службы Kaspersky Security в VMware NSX Manager.

3. Убедиться в том, что регистрация службы Kaspersky Security завершилась успешно (см. раздел "Просмотр зарегистрированных служб в консоли VMware vSphere Web Client" на стр. 57).

4. В консоли VMware vSphere Web Client настроить группу безопасности NSX (NSX Security Group) (см. раздел "Настройка группы безопасности NSX (NSX Security Group)" на стр. 58).

5. В консоли VMware vSphere Web Client настроить политику безопасности NSX (NSX Security Policy) и применить политику безопасности на группу или группы безопасности NSX (см. раздел "Настройка политики безопасности NSX (NSX Security Policy)" на стр. 59).

6. В консоли VMware vSphere Web Client развернуть SVM с компонентом Файловый Антивирус на гипервизорах VMware ESXi (см. раздел "Развертывание SVM с компонентом Файловый Антивирус" на стр. 60).

   После развертывания SVM Сервер интеграции передает на каждую новую SVM параметры конфигурации, которые вы указали при вводе параметров службы Kaspersky Security.

В этом разделе

Ввод параметров служб Kaspersky Security

После настройки подключения Сервера интеграции к серверу VMware vCenter вам требуется ввести параметры, необходимые для выполнения следующих процедур:

- регистрации в VMware NSX Manager службы Kaspersky Security;
- развертывания службы защиты файловой системы;
- первоначальной настройки конфигурации новых SVM после развертывания службы защиты файловой системы.

Регистрацию службы Kaspersky Security и настройку конфигурации новых SVM выполняет Сервер интеграции.

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

1. Запустите Консоль управления Сервера интеграции.
2. Перейдите на закладку **Защита виртуальной инфраструктуры**.
3. В списке выберите сервер VMware vCenter и разверните список доступных действий щелчком мыши по адресу или имени сервера VMware vCenter в графе **Адрес**.
4. В блоке **Управление защитой** выберите действие **Зарегистрировать службы Kaspersky Security**.

Запустится мастер ввода параметров, необходимых для регистрации и развертывания служб Kaspersky Security. Следуйте указаниям мастера.

В этом разделе

Шаг 1. 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.

Перейдите к следующему шагу мастера.

Сервер интеграции проверит возможность подключения к VMware NSX Manager с указанными параметрами.

Во время подключения Сервер интеграции 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 корневой сертификат цепочки сертификатов отсутствует или не является доверенным, вы можете устранить ошибку подключения путем добавления полученного сертификата в

список доверенных сертификатов. Для этого нажмите на кнопку **Считать доверенным**. Полученный сертификат будет установлен в качестве доверенного на компьютере, где установлена Консоль управления Сервера интеграции.

Шаг 2. Выбор образа SVM с компонентом Файловый Антивирус

На этом шаге укажите адрес, по которому расположен образ SVM с установленным компонентом Файловый Антивирус. Указанный образ будет развернут на гипервизорах в результате развертывания службы защиты файловой системы (Kaspersky File Antimalware Protection).

► *Чтобы указать адрес образа SVM, выполните следующие действия:*

1. Укажите адрес OVF-файла образа SVM с компонентом Файловый Антивирус на сетевом ресурсе, доступном по протоколу HTTP или HTTPS.

2. Нажмите на кнопку **Проверить**.

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

   Если проверка закончилась успешно, в нижней части окна отобразится следующая информация о выбранном образе 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.

Перейдите к следующему шагу мастера.

Шаг 3. Выбор образа SVM с компонентом Обнаружение сетевых угроз

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

На этом шаге откажитесь от установки компонента Обнаружение сетевых угроз. Для этого снимите флажок **Зарегистрировать службу сетевой защиты**.

Перейдите к следующему шагу мастера.

Шаг 4. Настройка параметров подключений для SVM и Сервера интеграции

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 следующие параметры:

- Параметры для подключения VMware NSX Manager к Серверу интеграции.
- Параметры для подключения SVM к Серверу интеграции.

По умолчанию для обоих подключений установлены параметры, которые Консоль управления Сервера интеграции получает из Kaspersky Security Center. В поле **Адрес** указано доменное имя компьютера, на котором установлен Сервер интеграции (если компьютер находится в домене), или имя компьютера в рабочей группе Windows (если компьютер не входит в домен).

Убедитесь, что VMware NSX Manager и SVM смогут подключиться к Серверу интеграции, используя параметры, установленные по умолчанию, или измените эти параметры.

Если требуется изменить установленные по умолчанию параметры для подключения VMware NSX Manager к Серверу интеграции, 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.

Если требуется изменить установленные по умолчанию параметры для подключения SVM к Серверу интеграции, 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.

Шаг 5. 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 журналам Kaspersky Security.

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

Пароль должен содержать от 8 до 128 символов. При создании паролей вы можете использовать буквы латинского алфавита, цифры, а также следующие символы: `! " ; % : ? * ( ) _ - + @ # $ ^ & \ / . , ' ` ~ < > { } [ ] | = №`.

Перейдите к следующему шагу мастера.

Шаг 6. Просмотр параметров служб Kaspersky Security

На этом шаге проверьте введенные параметры службы Kaspersky Security.

Перейдите к следующему шагу мастера, чтобы запустить регистрацию службы Kaspersky Security.

Шаг 7. Процесс регистрации служб Kaspersky Security

На этом шаге отображается информация о действиях, которые выполняет Сервер интеграции, чтобы зарегистрировать службу Kaspersky Security 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.

Шаг 8. Завершение работы мастера

На этом шаге отображается информация о результате регистрации службы Kaspersky Security.

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.

Подробную информацию об ошибках вы можете посмотреть в журналах Сервера интеграции:

- %ProgramData%\Kaspersky Lab\VIIS\logs\service.log – журнал работы Сервера интеграции;
- %ProgramData%\Kaspersky Lab\VIIS Console\logs\console.log – журнал работы Консоли управления Сервера интеграции.

Просмотр зарегистрированных служб в консоли VMware vSphere Web Client

Регистрацию службы Kaspersky Security 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/13172.

Настройка группы безопасности NSX (NSX Security Group)

Настройка групп безопасности NSX (NSX Security Group) выполняется в консоли VMware vSphere Web Client. Вам требуется включить в группу безопасности NSX все виртуальные машины, которые вы хотите защищать с помощью программы Kaspersky Security. Для этого требуется создать и настроить группу безопасности NSX.

► *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 имя 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 управления 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 управления VMware. При этом вы можете указать отдельные объекты управления VMware, 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/13172.

Настройка политики безопасности NSX (NSX Security Policy)

Настройка политики безопасности NSX (NSX Security Policy) выполняется в консоли VMware vSphere Web Client. Вам требуется назначить для ранее созданной группы безопасности NSX (NSX Security Group) политику безопасности NSX, в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

► *Чтобы настроить 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** выберите для политики действие **Apply Policy**. В открывшемся окне выберите группу безопасности

NSX, в которую включены защищаемые виртуальные машины, и нажмите на кнопку **OK**.

Подробнее о настройке политик безопасности NSX см. в Базе знаний http://support.kaspersky.ru/13172.

Развертывание SVM с компонентом Файловый Антивирус

SVM с компонентом Файловый Антивирус разворачиваются на гипервизорах VMware ESXi в результате развертывания службы Kaspersky Security (службы защиты файловой системы) на кластерах VMware. Развертывание службы выполняется в консоли VMware vSphere Web Client.

► *Чтобы развернуть SVM с компонентом Файловый Антивирус, 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 Файловый Антивирус будет развернута на каждом гипервизоре в составе кластера VMware, который вы выбрали.

   Подробнее о процедуре развертывания SVM с компонентом Файловый Антивирус см. в Базе знаний http://support.kaspersky.ru/13172.

Развертывание защиты в инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager

Для развертывания защиты в инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager требуется выполнить следующие действия:

1. В Консоли управления Сервера интеграции изменить пароль учетной записи svm, созданный автоматически во время установки Сервера интеграции (см. раздел "Изменение пароля учетной записи svm" на стр. 47). Пароль учетной записи svm требуется для настройки подключения SVM с установленным компонентом Файловый Антивирус к Серверу интеграции, который будет осуществлять взаимодействие между сервером VMware vCenter и SVM. Настройка подключения SVM к Серверу интеграции выполняется в ходе установки компонента Файловый Антивирус.

2. В Консоли управления Сервера интеграции настроить параметры подключения Сервера интеграции к одному или нескольким серверам VMware vCenter (см. раздел "Настройка параметров подключения Сервера интеграции к серверам VMware vCenter" на стр. 48).

3. Развернуть SVM с компонентом Файловый Антивирус на гипервизорах под управлением каждого сервера VMware vCenter.

► *Чтобы развернуть SVM с компонентом Файловый Антивирус, выполните следующие действия:*

1. Запустите Консоль управления Сервера интеграции (см. раздел "Запуск Консоли управления Сервера интеграции" на стр. 46).

2. Перейдите на закладку **Защита виртуальной инфраструктуры**.

3. В списке выберите сервер VMware vCenter и разверните список доступных действий щелчком мыши по адресу или имени сервера VMware vCenter в графе **Адрес**.

4. В блоке **Управление защитой** выберите действие **Управление SVM**. Откроется мастер управления SVM.

5. Выберите вариант **Развертывание** и перейдите к следующему шагу мастера.

6. Следуйте указаниям мастера.

В этом разделе

Шаг 1. Подключение к серверу VMware vCenter

На этом шаге укажите параметры подключения к серверу VMware vCenter:

- **Адрес сервера VMware vCenter**. IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера VMware vCenter, к которому производится подключение. По

умолчанию в поле указан адрес сервера VMware vCenter, который вы выбрали в Консоли управления Сервера интеграции.

- **Имя пользователя**. Имя учетной записи, под которой производится подключение к серверу VMware vCenter.
- **Пароль**. Пароль учетной записи, под которой производится подключение к серверу VMware vCenter.

> Требуется указать имя и пароль учетной записи администратора с правом на создание виртуальных машин.

Перейдите к следующему шагу мастера.

Во время подключения мастер проверяет SSL-сертификат, полученный от сервера VMware vCenter. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. Вы можете посмотреть информацию о полученном сертификате. Для этого 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 этому серверу VMware vCenter не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для сервера <адрес сервера VMware vCenter>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для сервера <адрес сервера VMware vCenter>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<адрес>\, где <адрес> – адрес сервера, от которого получен сертификат. При этом мастер проверяет наличие ранее установленного доверенного сертификата для этого сервера VMware vCenter. 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 VMware vCenter, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

Шаг 2. Ввод IP-адреса Сервера администрирования Kaspersky Security Center

Мастер получает из Kaspersky Security Center адрес, который будет использовать SVM для подключения к Серверу администрирования Kaspersky Security Center. Этот шаг доступен, если в качестве адреса для подключения к Серверу администрирования из Kaspersky Security Center передано NetBIOS-имя или DNS-имя компьютера. Если в качестве адреса для подключения передан IP-адрес компьютера, на котором установлен Сервер администрирования Kaspersky Security Center, этот шаг пропускается.

Укажите IP-адрес компьютера, на котором установлен Сервер администрирования Kaspersky Security Center. IP-адрес указывается в формате IPv4.

Перейдите к следующему шагу мастера.

Шаг 3. Выбор файла образа SVM

На этом шаге укажите файл образа SVM с установленным компонентом Файловый Антивирус. Для этого нажмите на кнопку **Обзор** и в открывшемся окне выберите OVF-файл образа SVM.

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

Если проверка закончилась успешно, в нижней части окна отобразится следующая информация о выбранном образе SVM:

- **Название программы** – название программы, которая установлена на SVM.
- **Версия программы** – номер версии программы.
- **Версия SVM** – номер версии SVM.

- **Производитель** – производитель программы, которая установлена на SVM.
- **Описание** – краткое описание программы.
- **Издатель** – издатель сертификата, которым подписан образ SVM.
- **Размер образа** – размер образа SVM.
- **Размер на диске** – примерный объем дискового пространства, которое требуется для развертывания SVM в хранилище данных гипервизора VMware ESXi:
  - при динамическом выделении дискового пространства с использованием VMware vStorage Thin Provisioning;
  - при выделении дискового пространства с неизменяемым объемом.

Перейдите к следующему шагу мастера.

Шаг 4. Выбор гипервизоров VMware ESXi

На этом шаге выберите гипервизоры VMware ESXi, на которые вы хотите развернуть SVM.

В графах таблицы отображается информация обо всех гипервизорах VMware ESXi под управлением одного сервера VMware vCenter:

- **Гипервизор VMware ESXi** – IP-адрес или доменное имя гипервизора.
- **Состояние** – текущее состояние гипервизора: доступен, не доступен.
- **SVM** – информация о наличии SVM на гипервизоре:
  - **Развернута** – на гипервизоре развернута SVM, виртуальные машины этого гипервизора защищены.
  - **Не развернута** – на гипервизоре не развернута SVM, виртуальные машины этого гипервизора не защищены.

Вы можете выбирать те доступные по сети гипервизоры VMware ESXi, на которых не развернута SVM.

Чтобы выбрать гипервизор, установите в таблице флажок слева от названия этого гипервизора.

Перейдите к следующему шагу мастера.

Шаг 5. Выбор варианта размещения и настройка параметров развертывания

На этом шаге выберите вариант размещения SVM в хранилище данных гипервизора VMware ESXi:

- **Динамическое выделение с использованием VMware vStorage Thin Provisioning**. Во время выделения пространства в хранилище данных гипервизора для SVM резервируется минимально необходимый объем. При необходимости этот объем увеличивается. Этот вариант выбран по умолчанию.
- **Выделение дискового пространства с неизменяемым объемом**. Во время выделения пространства в хранилище данных гипервизора для SVM сразу резервируется требуемый объем.

Настройте параметры процесса развертывания SVM. Если вы хотите, чтобы мастер развертывал SVM одновременно на нескольких гипервизорах VMware ESXi, установите флажок **Разрешить параллельное развертывание**. В поле **Развертывать одновременно не более чем на N гипервизорах VMware ESXi** укажите количество гипервизоров, на которых SVM требуется развертывать одновременно.

Перейдите к следующему шагу мастера.

Шаг 6. Выбор хранилища данных

На этом шаге для каждой SVM выберите хранилище данных из списка хранилищ данных, подключенных к гипервизорам VMware ESXi.

В графах таблицы отображается следующая информация:

- **Гипервизор VMware ESXi** – IP-адрес или доменное имя гипервизора.

- **Имя SVM** – имя SVM, которая будет размещена на этом гипервизоре. SVM автоматически присваивается имя ksv-<N>, где N – IP-адрес или доменное имя гипервизора VMware ESXi, на котором размещена SVM. Например, ksv-192-168-0-2 или ksv-esx-avp-ru.

  Вы можете изменить имя SVM. Для этого щелкните левой клавишей мыши по графе **Имя SVM** и введите новое имя.

  > При вводе имени SVM вы можете использовать буквы латинского алфавита, цифры и дефис. Имя SVM не может начинаться с дефиса и заканчиваться дефисом.

- **Хранилище данных** – в раскрывающемся списке отображаются имена хранилищ данных, соответствующих тому варианту размещения SVM, который вы выбрали на предыдущем шаге. По умолчанию в списке выбрано хранилище, в котором достаточно места для развертывания SVM. Если на гипервизоре отсутствуют хранилища данных, соответствующие выбранному варианту размещения SVM, мастер отображает сообщение об этом.

В раскрывающемся списке графы **Хранилище данных** для каждой SVM выберите хранилище данных.

Перейдите к следующему шагу мастера.

Шаг 7. Настройка соответствия виртуальных сетей

На этом шаге установите соответствие виртуальных сетей SVM и гипервизора VMware ESXi:

- В графе **Гипервизор VMware ESXi** отображается IP-адрес или доменное имя гипервизора, на котором разворачивается SVM.

- В графе **Сеть VMware vShield** в раскрывающемся списке выберите виртуальную сеть гипервизора VMware ESXi, которую SVM должна использовать для связи с компонентом VMware vShield Endpoint ESX Module. Этот компонент установлен на

гипервизоре VMware ESXi. Компонент обеспечивает взаимодействие драйвера VMware NSX File Introspection, установленного на виртуальной машине, и SVM.

- В графе **Сеть управления** в раскрывающемся списке выберите виртуальную сеть гипервизора VMware ESXi, которую SVM должна использовать для связи с внешним сетевым окружением и Сервером администрирования Kaspersky Security Center.

Перейдите к следующему шагу мастера.

Шаг 8. Ввод сетевых параметров

На этом шаге укажите сетевые параметры SVM:

- **Использовать DHCP**. Используется сетевой протокол DHCP, который позволяет SVM автоматически получать сетевые параметры. Этот вариант выбран по умолчанию.
- **Распределять, используя заданные параметры**. Сетевые параметры назначаются SVM вручную, исходя из заданного диапазона. Если вы выбрали этот вариант, укажите следующие параметры сети:
  - Начальный IP-адрес из диапазона адресов, начиная с которого SVM автоматически присваиваются IP-адреса. Конечный IP-адрес диапазона определяется автоматически, исходя из количества разворачиваемых SVM.
  - Шлюз по умолчанию.
  - DNS-сервер. Вы можете указать один или два DNS-сервера через запятую.
  - Маска подсети.

Перейдите к следующему шагу мастера.

Шаг 9. Распределение сетевых параметров

Этот шаг доступен, если на предыдущем шаге мастера вы выбрали параметр **Распределять, используя заданные параметры**. Если вы выбрали параметр **Использовать DHCP**, этот шаг пропускается.

В таблице отображаются сетевые параметры SVM, которые вы указали на предыдущем шаге. Вы можете изменить значения параметров для определенных SVM или ввести параметры, не указанные на предыдущем шаге.

Перейдите к следующему шагу мастера.

Шаг 10. 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 журналам Kaspersky Security.

Пароль должен содержать от 8 до 128 символов. При создании паролей вы можете использовать буквы латинского алфавита, цифры, а также следующие символы: ! " ; % : ? * ( ) _ - + @ # $ ^ & \ / . , ' ` ~ < > { } [ ] | = №.

Для предотвращения несанкционированного доступа к SVM рекомендуется регулярно изменять пароль конфигурирования. Вы можете изменить пароль конфигурирования с помощью процедуры изменения конфигурации SVM.

Перейдите к следующему шагу мастера.

Шаг 11. Ввод параметров подключения к VMware vShield Manager

Для регистрации SVM в VMware vShield Manager мастер выполняет подключение к VMware vShield Manager.

На этом шаге укажите параметры подключения к VMware vShield Manager:

- **Адрес VMware vShield Manager**. IP-адрес в формате IPv4 или полное доменное имя (FQDN) компонента VMware vShield Manager, в зоне действия которого находятся SVM.
- **Имя пользователя**. Имя учетной записи администратора для подключения к VMware vShield Manager.
- **Пароль**. Пароль учетной записи администратора для подключения к VMware vShield Manager.

Перейдите к следующему шагу мастера.

Мастер проверяет SSL-сертификат, полученный от VMware vShield Manager. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. Вы можете посмотреть информацию о полученном сертификате. Для этого 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 этому VMware vShield Manager не получать сообщение об ошибке сертификата. Для этого установите флажок **Установить полученный сертификат и больше не показывать предупреждения для сервера <адрес VMware vShield Manager>**.

Чтобы продолжить подключение, нажмите на кнопку **Продолжить** в окне **Проверка сертификата**. Если вы установили флажок **Установить полученный сертификат и больше не показывать предупреждения для сервера <адрес VMware vShield Manager>**, полученный сертификат сохраняется в реестре операционной системы на компьютере, где установлена Консоль администрирования Kaspersky Security Center, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStora

ge\<адрес>\, где <адрес> – адрес VMware vShield Manager, от которого получен сертификат. При этом мастер проверяет наличие ранее установленного доверенного сертификата для этого VMware vShield Manager. 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 VMware vShield Manager, и продолжить подключение, нажмите на кнопку **Да** в этом окне.

Мастер проверит наличие установленного компонента VMware vShield Endpoint на всех гипервизорах, на которых требуется развернуть SVM, и наличие лицензии на VMware vShield Endpoint. Если компонент не установлен или лицензия отсутствует, мастер сообщит об этом на следующем шаге.

Шаг 12. Ввод параметров подключения SVM к Серверу интеграции

На этом шаге укажите параметры подключения SVM к Серверу интеграции. Сервер интеграции осуществляет взаимодействие между сервером VMware vCenter и SVM и используется для получения информации о виртуальной инфраструктуре.

- **Адрес** – IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера интеграции.
- **Имя пользователя** – имя учетной записи, под которой производится подключение SVM к Серверу интеграции: *svm*.
- **Пароль** – пароль учетной записи, под которой производится подключение SVM к Серверу интеграции.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к Серверу интеграции с именем и паролем указанной учетной записи. Если у учетной записи недостаточно прав, мастер сообщит об этом и останется на текущем шаге.

Во время подключения мастер проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. 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, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<адрес>\, где <адрес> – адрес Сервера интеграции, от которого получен сертификат. 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.

Шаг 13. Запуск развертывания SVM

Все параметры, необходимые для развертывания SVM, были введены.

Перейдите к следующему шагу мастера, чтобы запустить развертывание SVM.

Шаг 14. Развертывание SVM

На этом шаге выполняется развертывание SVM на гипервизорах VMware ESXi. Процесс занимает некоторое время. Дождитесь завершения развертывания.

Информация о процессе развертывания SVM отображается в таблице. Время начала и окончания процесса развертывания на каждом гипервизоре отображается в графах **Начало** и **Окончание**. Эта информация позволяет оценить время, необходимое для развертывания всех SVM.

Если в ходе развертывания SVM на гипервизоре происходит ошибка, мастер выполняет откат внесенных изменений на этом гипервизоре и отменяет регистрацию SVM в VMware vShield Manager, если регистрация была выполнена. Развертывание SVM на других гипервизорах продолжается.

После развертывания SVM автоматически включается.

Перейдите к следующему шагу мастера.

Шаг 15. Завершение установки компонента Файловый Антивирус

На этом шаге отображается информация о результатах развертывания SVM на гипервизорах VMware ESXi.

Завершите работу мастера.

Если развертывание SVM завершилось с ошибкой, мастер отображает ссылку на файл журнала работы мастера. Вы можете использовать этот файл при обращении в Службу технической поддержки.

Подготовка программы к работе

После установки программы требуется выполнить следующие действия:

- Активировать программу на всех новых SVM (см. раздел "Процедура активации программы" на стр. 77).
- Обновить базы программы на всех новых SVM (см. раздел "Процедура обновления баз программы" на стр. 79).
- Создать политику, которая будет применяться на SVM (см. раздел "Создание политики" на стр. 81).

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 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 **Дополнительно** / **Управление программами** дерева консоли, во вложенной папке **Лицензии на ПО Лаборатории Касперского**;
- 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 *серверные или настольные ключи* (в зависимости от 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.

Если вы используете схему лицензирования по количеству защищенных виртуальных машин, тип ключа, с помощью которого вы активируете программу, должен соответствовать гостевой операционной системе виртуальных машин:

- для защиты виртуальных машин с серверной операционной системой нужно добавить на SVM серверный ключ;
- для защиты виртуальных машин с настольной операционной системой нужно добавить на SVM настольный ключ;
- для защиты виртуальных машин и с серверной, и с настольной операционной системой нужно добавить на SVM два ключа: серверный и настольный.

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

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 ключ в хранилище ключей Kaspersky Security Center:

   a. Откройте Консоль администрирования Kaspersky Security Center.

b. В дереве консоли в папке **Дополнительно** / **Управление программами** выберите вложенную папку **Лицензии на ПО Лаборатории Касперского**.

c. Нажмите на кнопку **Добавить ключ** в рабочей области. Запустится мастер добавления ключа в хранилище.

d. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.

e. На следующем шаге мастера, укажите путь к файлу ключа. Для этого нажмите на кнопку **Обзор** и в открывшемся окне выберите файл с расширением key.

f. Снимите флажок **Автоматически распространять ключ на управляемые устройства** (возможность автоматического распространения ключей не поддерживается для программы Kaspersky Security). Перейдите к следующему шагу мастера.

g. Завершите работу мастера добавления ключа в хранилище.

Добавленный ключ отобразится в списке ключей в папке **Дополнительно** / **Управление программами** дерева консоли, во вложенной папке **Лицензии на ПО Лаборатории Касперского**.

2. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.

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

В рабочей области выберите закладку **Задачи** и нажмите на кнопку **Создать задачу**. Запустится мастер создания задачи.

3. Укажите программу, для которой создается задача, и тип задачи. Для этого в списке **Kaspersky Security для виртуальных сред 4.0 Защита без агента** выберите **Активация программы**.

4. На следующем шаге мастера выберите ключ из хранилища ключей Kaspersky Security Center. Для этого нажмите на кнопку **Выбрать**. Откроется окно **Выбор ключа**. Выберите ключ и нажмите на кнопку **ОК**.

5. На следующем шаге мастера 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**.

6. На следующем шаге мастера введите имя 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 "Запуск, остановка и просмотр результатов запуска задач" на стр. 98).

Процедура обновления баз программы

► *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. 167). 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. Дождитесь запуска по расписанию задачи обновления баз программы или запустите задачу вручную.

   Задача обновления баз программы создается 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. 168).

4. 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. 186). Если на SVM отсутствуют базы программы, Kaspersky Security не защищает виртуальные машины.

Создание политики

После установки Kaspersky Security требуется настроить параметры работы программы с помощью политики. Если на SVM не применяется политика, Kaspersky Security не защищает виртуальные машины.

► *Чтобы создать политику, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для которого вы хотите создать политику.
3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Создать политику**, чтобы запустить мастер создания политики.
5. Следуйте указаниям мастера создания политики.

В этом разделе

Шаг 1. Выбор программы для создания групповой политики

На этом шаге в списке **Название программы** выберите **Kaspersky Security для виртуальных сред 4.0 Защита без агента**.

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Определение названия групповой политики для программы

На этом шаге в поле **Имя** введите имя политики.

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Настройка параметров корневого профиля защиты

После создания политики корневой профиль защиты назначается всем виртуальным машинам в составе защищаемой инфраструктуры кластера KSC. Значения параметров корневого профиля защиты, установленные по умолчанию, соответствуют рекомендациям специалистов "Лаборатории Касперского".

Значения параметров, установленные по умолчанию, достаточны для первоначальной настройки программы. Во время работы с программой вы можете выполнить более тонкую настройку параметров корневого профиля защиты (см. раздел "Параметры корневого профиля защиты" на стр. 104).

Перейдите к следующему шагу мастера создания политики.

Шаг 4. Параметры SNMP-мониторинга

Включение SNMP-мониторинга состояния SVM с компонентом Файловый Антивирус приводит к выходу программы из сертифицированного состояния.

По умолчанию SNMP-мониторинг отключен.

Перейдите к следующему шагу мастера создания политики.

Шаг 5. Соглашение об участии в Kaspersky Security Network

На этом шаге вам предлагается принять участие в программе Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 173).

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

В зависимости от расположения инфраструктуры различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского".
- Локальный KSN (Kaspersky Private Security Network) – инфраструктура расположена на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера.

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN.

Если вы хотите использовать в работе программы Локальный KSN, установите флажок **Использовать Локальный KSN, если он настроен в Kaspersky Security Center**.

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

Перейдите к следующему шагу мастера создания политики.

Шаг 6. Создание групповой политики для программы

Завершите работу мастера создания политики.

Окно мастера создания политики закроется. Созданная политика отобразится в списке политик на закладке **Политики**.

После того как Kaspersky Security Center передаст информацию программе Kaspersky Security, политика распространится на SVM. Kaspersky Security начнет защищать виртуальные машины на гипервизорах в соответствии с назначенным им корневым профилем защиты.

> Если на SVM не добавлен ключ или отсутствуют базы программы, Kaspersky Security не защищает виртуальные машины.

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.

► *Чтобы убедиться, что установка программы завершилась успешно, выполните следующие действия:*

1. Убедитесь, что на компьютере, где установлена Консоль администрирования Kaspersky Security Center, в списке установленных программ операционной системы отображается **Kaspersky Security для виртуальных сред 4.0 Защита без агента – компоненты управления**.

2. Убедитесь, что 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.

3. Убедитесь, что в Консоли администрирования Kaspersky Security Center в блоке **Развертывание** отображается ссылка для запуска Консоли управления Сервера интеграции. При переходе по ссылке запускается Консоль управления Сервера интеграции. После ввода параметров подключения происходит подключение к Серверу интеграции.

4. Убедитесь, что в Консоли администрирования Kaspersky Security Center в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center присутствует плагин управления Kaspersky Security (см. раздел "Установка плагина управления Kaspersky Security и Сервера интеграции" на стр. 43).

5. В консоли VMware vSphere Web Client в корневом дереве элементов выберите раздел **Hosts and Clusters** и убедитесь, что SVM успешно развернуты и находятся в состоянии **Powered On**.

6. В консоли VMware vSphere Web Client проверьте **Health status** службы **Kaspersky File Antimalware Protection**. Ожидаемый результат: **Installation status** = **Succeeded**, **Service status** = **UP**.

7. Убедитесь, что в Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** дерева консоли присутствует группа администрирования, которой присвоено имя сервера VMware vCenter.

8. Проверьте, что все развернутые SVM добавлены в эту группу администрирования.

9. Убедитесь, что в Консоли администрирования Kaspersky Security Center задача активации и задача обновления баз программы завершены успешно на всех развернутых SVM. Список задач отображается на закладке **Задачи** в рабочей области группы администрирования, которой присвоено имя сервера VMware vCenter. Вы можете посмотреть результаты выполнения задачи по ссылке **Посмотреть результаты**, расположенной справа от списка задач.

10. В Консоли администрирования Kaspersky Security Center откройте группу администрирования, которой присвоено имя сервера VMware vCenter, и убедитесь, что на закладке **Политики** присутствует политика в статусе **Активна**.

11. В Консоли администрирования Kaspersky Security Center откройте группу администрирования, которой присвоено имя сервера VMware vCenter, и убедитесь, что на закладке **Устройства** все SVM имеют статус **ОК** (зеленый).

12. Для каждой SVM на закладке **Устройства** откройте окно статистики. Для этого в окне свойств SVM выберите раздел **Программы**, затем выберите в списке программу Kaspersky Security для виртуальных сред 4.0 Защита без агента и нажмите на кнопку **Статистика**. Убедитесь, что отображается информация о лицензии и базах программы.

13. В Консоли администрирования Kaspersky Security Center перейдите в папку группы администрирования, которой присвоено имя сервера VMware vCenter, и откройте список всех виртуальных машин, находящихся под управлением этого сервера VMware vCenter. Для этого выберите вложенную папку **Кластеры и массивы серверов**, в рабочей области выберите кластер KSC, откройте окно свойств выбранного кластера KSC и выберите раздел **Список виртуальных машин**. Убедитесь, что все виртуальные машины защищаются.

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. 77).
- Базы программы обновлены на всех SVM (см. раздел "Процедура обновления баз программы" на стр. 79).
- Настроена активная политика, которая применяется на всех SVM (см. раздел "Создание политики" на стр. 81).
- Настроена задача полной проверки для всех SVM (см. раздел "Создание задачи полной проверки" на стр. 130).
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированном состоянии" на стр. 194).

Проверка работоспособности. Тестовый файл EICAR

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе (см. раздел "Процедура приемки" на стр. 85).

- Программа находится в сертифицированном состоянии (см. раздел "Сертифицированное состояние программы" на стр. 87).
- На виртуальной машине установлен драйвер VMware NSX File Introspection.
- 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. Отключите защиту виртуальной машины:
   a. Откройте свойства политики, под управлением которой находится SVM, защищающая виртуальную машину.
   b. Перейдите в раздел **Корневой профиль защиты** и снимите флажок **Включить защиту**.

   > 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, под управлением которой находится SVM, защищающая виртуальную машину.

   b. Перейдите в раздел **Корневой профиль защиты** и установите флажок **Включить защиту**.

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 ошибку 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 о вирусах**. 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. Отключите защиту виртуальной машины:

   a. Откройте свойства политики, под управлением которой находится SVM, защищающая виртуальную машину.

   b. Перейдите в раздел **Корневой профиль защиты** и снимите флажок **Включить защиту**.

   > 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 списке **Действие при обнаружении угрозы** выбрано одно из следующих значений:

   - **Выбирать действие автоматически**;
   - **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 о вирусах**. 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).

Концепция управления программой через Kaspersky Security Center

Управление программой Kaspersky Security для виртуальных сред 4.0 Защита без агента осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center. В случае программы Kaspersky Security для виртуальных сред 4.0 Защита без агента клиентским компьютером Kaspersky Security Center является SVM. Защищенные виртуальные машины не являются клиентскими компьютерами с точки зрения Kaspersky Security Center, так как на них не устанавливается Агент администрирования Kaspersky Security Center.

SVM, развернутые на гипервизорах VMware ESXi под управлением одного сервера VMware vCenter, в Kaspersky Security Center объединяются в *кластер KSC* (кластер Kaspersky Security Center). Кластеру KSC присваивается имя соответствующего сервера VMware vCenter. Объекты управления VMware под управлением этого сервера VMware vCenter образуют *защищаемую инфраструктуру* кластера KSC.

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

- *Политика* применяется на SVM и определяет параметры защиты виртуальных машин от вирусов и других программ, представляющих угрозу, и параметры резервных хранилищ на SVM.

  В случае программы Kaspersky Security для виртуальных сред 4.0 Защита без агента политика может применяться на всех SVM одного кластера KSC или на всех SVM всех кластеров KSC, входящих в группу администрирования. Политика определяет параметры защиты всех виртуальных машин в составе защищаемой инфраструктуры кластера KSC, на SVM которого применяется политика.

- *Задачи* 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 политике Kaspersky Security и профилях защиты

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

Параметры защиты виртуальных машин в политике определяются *профилем защиты*. Во время создания политики формируется *корневой профиль защиты*. Корневой профиль защиты назначается корневому объекту в структуре объектов управления VMware – серверу VMware vCenter. В соответствии с порядком наследования профилей защиты, все объекты управления VMware, в том числе и виртуальные машины в составе защищаемой инфраструктуры кластера KSC, наследуют корневой профиль защиты, если им не назначен собственный профиль защиты. Таким образом, всем виртуальным машинам в составе защищаемой инфраструктуры кластера KSC назначаются одинаковые значения параметров защиты.

Корневой профиль защиты недоступен для удаления, однако вы можете изменять значения параметров корневого профиля.

После создания политики вы можете создать *дополнительные профили защиты* (далее "профили защиты"). Благодаря профилям защиты вы можете гибко настроить разные параметры защиты для разных виртуальных машин. Политика может включать несколько профилей защиты. Профиль защиты назначается объектам управления VMware в составе защищаемой инфраструктуры кластера KSC. Одному объекту управления VMware может быть назначен только один профиль защиты.

Kaspersky Security защищает виртуальную машину с теми параметрами, которые указаны в назначенном виртуальной машине профиле защиты.

В профиле защиты вы можете настроить 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).

После создания политики вы можете настроить следующие параметры работы программы в свойствах политики:

- параметры резервного хранилища;
- параметры использования KSN (см. раздел "Участие в Kaspersky Security Network" на стр. 173).

Параметры и блоки параметров политики имеют атрибут "замок" –  "Замок" показывает, наложен ли запрет на изменение параметров в политиках вложенного уровня иерархии (для вложенных групп администрирования и подчиненных Серверов администрирования) и в параметрах задач. Если в политике для параметра или блока параметров установлен "замок", переопределить значение этих параметров невозможно (см. в документации Kaspersky Security Center).

Kaspersky Security Center позволяет задавать сложную иерархию групп администрирования и политик (подробнее см. в документации Kaspersky Security Center). В программе Kaspersky Security каждая политика получает сведения о виртуальной инфраструктуре от Сервера интеграции, который подключается к определенному серверу VMware vCenter. Если вы используете сложную иерархию групп администрирования и политик, политика нижнего уровня наследует некорректные параметры получения сведений о виртуальной инфраструктуре. Поэтому во время настройки параметров Kaspersky Security рекомендуется не задавать сложную иерархию групп администрирования и политик, а создавать отдельную политику для группы администрирования, которая содержит кластер KSC.

Kaspersky Security использует наследование профилей защиты согласно иерархии объектов управления VMware.

Профиль защиты, назначенный объекту управления VMware, наследуется всеми его дочерними объектами, в том числе и виртуальными машинами, если дочернему объекту / виртуальной машине не назначен собственный профиль защиты (см. раздел "Назначение виртуальной машине профиля защиты" на стр. 120) или если дочерний объект / виртуальная машина не исключены из защиты (см. раздел "Выключение защиты на виртуальной машине" на стр. 124). Таким образом, вы можете назначить виртуальной машине собственный профиль защиты или использовать для нее профиль защиты, унаследованный от родительского объекта.

Объект управления VMware может быть исключен из защиты. Если вы исключаете объект управления VMware 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 виртуальным машинам в составе кластера VMware или ресурсного пула.

О задачах Kaspersky Security

Kaspersky Security Center управляет работой программы Kaspersky Security с помощью задач. Задачи реализуют основные функции программы, например проверку виртуальных машин или обновление баз программы.

Для управления программой Kaspersky Security вы можете использовать следующие задачи:

- **Полная проверка**. Задача запускается на SVM и позволяет проверять на вирусы и другие программы, представляющие угрозу, все виртуальные машины, которые находятся под защитой этих SVM. Вы можете создать задачу полной проверки для SVM одного кластера KSC, SVM всех кластеров KSC, входящих в группу администрирования, или для отдельной SVM.

- **Выборочная проверка**. Kaspersky Security проверяет на вирусы и другие программы, представляющие угрозу, выбранные виртуальные машины, которые находятся под защитой SVM одного кластера KSC. Задача выборочной проверки позволяет проверять виртуальные машины, находящиеся под управлением одного сервера VMware vCenter.

- **Обновление**. Kaspersky Security Center устанавливает обновления баз программы на SVM, на которых запускается задача. Вы можете создать задачу обновления для SVM одного кластера KSC, SVM всех кластеров KSC, входящих в группу администрирования, или для отдельной SVM.

- **Откат обновления**. Kaspersky Security Center откатывает последнее обновление баз программы на SVM, на которых запускается задача. Вы можете создать задачу отката обновления для SVM одного кластера KSC, SVM всех кластеров KSC, входящих в группу администрирования, или для отдельной SVM.

- **Активация программы**. Kaspersky Security Center добавляет на SVM, на которых запускается задача, ключ для активации программы или для продления срока действия лицензии. Вы можете создать задачу активации программы для SVM одного кластера KSC, SVM всех кластеров KSC, входящих в группу администрирования, или для отдельной SVM.

Для работы с программой Kaspersky Security через Kaspersky Security Center вы можете создавать задачи следующих типов:

- *Групповая задача* – задача, которая выполняется на клиентских компьютерах выбранной группы администрирования. Применительно к программе Kaspersky Security групповые задачи могут выполняться на SVM одного кластера KSC или на SVM всех кластеров KSC, входящих в группу администрирования.

- *Задача для набора компьютеров* – задача для одной или нескольких SVM, как входящих, так и не входящих в группы администрирования.

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

Запуск, остановка и просмотр результатов запуска задач

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Если вы хотите запустить или остановить задачу, созданную для SVM всех кластеров KSC, в дереве консоли выберите папку **Управляемые устройства**. В рабочей области выберите закладку **Задачи**.

   - Если вы хотите запустить или остановить задачу, созданную для SVM одного или нескольких кластеров KSC, входящих в одну группу администрирования, в папке **Управляемые устройства** выберите папку с названием этой группы администрирования. В рабочей области выберите закладку **Задачи**.

   - Если вы хотите запустить или остановить задачу, созданную для одной или нескольких SVM, выберите папку **Задачи** дерева консоли.

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.

Вы можете посмотреть информацию о ходе и результатах выполнения задач 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 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**.

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. Для полноценной работы с программой Kaspersky Security пользователь должен обладать правами роли "Главный администратор".

По умолчанию роль "Главный администратор" назначается пользователям, входящим в одну из следующих групп:

- KLAdmins.
- Администраторы (локальные администраторы компьютеров, на которых установлен Сервер администрирования Kaspersky Security Center).

Для пользователей, которые не обладают правами роли "Главный администратор", 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.

Файловый Антивирус. Защита виртуальных машин

SVM с установленным компонентом Файловый Антивирус обеспечивает защиту виртуальных машин на гипервизоре VMware ESXi. Kaspersky Security начинает защищать виртуальные машины только после того, как вы настроили параметры работы программы с помощью политики (см. раздел "Создание политики" на стр. 81). Kaspersky Security защищает виртуальные машины с теми параметрами, которые указаны в назначенных им профилях защиты (см. раздел "О политике Kaspersky Security и профилях защиты" на стр. 94).

Если на SVM программа не активирована (см. раздел "Процедура активации программы" на стр. 77) или отсутствуют базы программы (см. раздел "Процедура обновления баз программы" на стр. 79), Kaspersky Security не защищает виртуальные машины.

Kaspersky Security защищает виртуальные машины, которые соответствуют следующим требованиям:

- В инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager:
  - Виртуальная машина не выключена и не приостановлена.

    Kaspersky Security может проверять выключенные виртуальные машины с файловой системой NTFS или FAT32 при выполнении задач проверки.
  - На виртуальной машине с операционной системой Windows установлен и включен драйвер VMware NSX File Introspection.
  - На виртуальной машине с операционной системой Linux установлен и включен драйвер VMware Linux Thin Agent.

Kaspersky Security защищает виртуальные машины с операционными системами Linux, только если вы используете платформу VMware NSX for vSphere версии 6.3.1.

- Виртуальная машина входит в состав группы безопасности NSX (NSX Security Group), настроенной в консоли VMware vSphere Web Client. Для этой группы назначена политика безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).
- В профиле защиты, который назначен виртуальной машине, включена защита.

- В инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager:
  - Виртуальная машина не выключена и не приостановлена.
  - На виртуальной машине установлен и включен драйвер VMware NSX File Introspection.
  - В профиле защиты, который назначен виртуальной машине, включена защита.

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

Когда пользователь или программа обращается к файлу виртуальной машины, 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 используются сигнатурный и эвристический анализ. При *сигнатурном анализе* используются базы Kaspersky Security, содержащие информацию об известных угрозах и о методах их устранения. Защита с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

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 маши (см. раздел "Выключение защиты на виртуальной машине" на стр. 124)н.

В этом разделе

Параметры корневого профиля защиты

Изменение значений некоторых параметров корневого профиля защиты 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. 194).

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

Для настройки доступны следующие параметры корневого профиля защиты:

1. **Включить защиту**

   Включение / выключение функции защиты.

   Если флажок установлен, Kaspersky Security проверяет все открываемые, сохраняемые и запускаемые файлы на виртуальных машинах, которым назначен профиль защиты.

   Если флажок снят, программа не защищает виртуальные машины, которым назначен профиль защиты.

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

   По умолчанию флажок установлен.

   Выключение функции защиты приводит к выходу программы из сертифицированного состояния.

2. В блоке **Уровень безопасности** вы можете установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**) или настроить уровень безопасности самостоятельно:

   - 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**. Откроется окно **Параметры уровня безопасности**.

   a. В блоке **Проверка архивов и составных файлов** вы можете настроить следующие параметры:

- **Проверять архивы**

  Включение / выключение проверки архивов.

  По умолчанию флажок снят.

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

  Удаление 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**.

  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** вы можете настроить следующие параметры:

- **Ограничивать время 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** вы можете выбрать объекты, которые будет обнаруживать Kaspersky Security. Для этого нажмите на кнопку **Настройка** и укажите объекты в открывшемся окне:

- **Вредоносные утилиты**

Включение / выключение защиты от вредоносных утилит.

Вредоносные утилиты не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. 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 других легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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 или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нанесения вреда компьютеру или данным пользователя.

Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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.

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

3. В блоке **Действие при обнаружении угрозы** вы можете выбрать действие, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы:

   - **Выбирать действие автоматически**

     Kaspersky Security выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию. Это действие **Лечить. Удалять, если лечение невозможно**.

     Этот вариант действия выбран по умолчанию.

   - **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 установлен флажок **Удалять архивы, если лечение не удалось** в параметрах уровня безопасности.

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

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

   - **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.

4. В блоке **Область защиты** вы можете отменить проверку файлов на сетевых дисках во время защиты виртуальных машин с операционными системами Windows. Для этого снимите флажок **Проверять сетевые диски**. 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.

5. В блоке **Исключения из защиты** вы можете исключить из защиты какие-либо файлы виртуальных машин. Для этого нажмите на кнопку **Настройка**. Откроется окно **Исключения из защиты**.

   a. В блоке **Расширения файлов** вы можете выбрать один из следующих вариантов:

   - **Проверять все, кроме файлов со следующими расширениями**. Если вы выбрали этот вариант, 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**. Если вы выбрали этот вариант, 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. При указании расширений файлов вы можете использовать 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** вы можете сформировать список объектов, которые требуется исключить из защиты, с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

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 корневой 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 `?`.

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".

> В списке исключений не поддерживается использование переменных окружения. Объект файловой системы, заданный с использованием переменных окружения, не исключается из защиты. Если вы импортировали список исключений, который содержит переменные окружения, вам требуется заменить их абсолютными значениями.

Во время защиты виртуальных машин с операционными системами Windows программа Kaspersky Security игнорирует регистр символов в путях к файлам и папкам на локальных устройствах. В сетевых путях к файлам и папкам, исключаемым из защиты на виртуальных машинах с операционными системами Windows, регистр символов также по умолчанию игнорируется. Если вы хотите задавать сетевые пути на виртуальных машинах с операционными системами Windows с учетом регистра символов, установите флажок **Учитывать регистр символов в сетевых путях**.

Во время защиты виртуальных машин с операционными системами Linux программа Kaspersky Security всегда игнорирует регистр символов в путях к файлам и директориям во всех поддерживаемых файловых системах (локальных и сетевых).

Просмотр защищаемой инфраструктуры кластера KSC

► *Чтобы просмотреть защищаемую инфраструктуру кластера KSC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC.

3. В рабочей области выберите закладку **Политики**.

4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.

5. В окне **Свойства: <Название политики>** выберите раздел **Защищаемая инфраструктура**.

6. В правой части окна нажмите на кнопку **Подключить**.

   Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, плагин управления Kaspersky Security пытается автоматически подключиться к Серверу интеграции под доменной учетной записью текущего пользователя.

   > Убедитесь, что ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции.

7. Если установить подключение не удалось или компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен, откроется окно **Параметры подключения к Серверу интеграции**.

   Укажите параметры подключения:

   - 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, вы можете использовать вашу доменную учетную запись для подключения к Серверу интеграции. 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 сохраненный пароль администратора отображается в окне ввода параметров подключения.

8. Нажмите на кнопку **ОК** в окне **Параметры подключения к Серверу интеграции**.

Плагин управления Kaspersky Security проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно **Проверка сертификата** с сообщением об ошибке. 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, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<адрес>\, где <адрес> – адрес Сервера интеграции, от которого получен сертификат. 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.

9. Откроется окно **Список серверов VMware vCenter**. Выберите сервер VMware vCenter, соответствующий кластеру KSC, защищаемую инфраструктуру которого вы хотите посмотреть, и нажмите на кнопку **ОК**.

Информация о защищаемой инфраструктуре кластера KSC

В правой части окна отобразится защищаемая инфраструктура кластера KSC: сервер VMware vCenter, объекты Datacenter, кластеры VMware, ресурсные пулы, объекты vApp и виртуальные машины. Kaspersky Security использует отображение защищаемой инфраструктуры кластера KSC в виде дерева гипервизоров VMware ESXi и кластеров VMware (Hosts and Clusters view) (подробнее см. в документации к продуктам VMware).

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 профилях защиты

В графе **Профиль защиты** отображается название профиля защиты, с параметрами которого Kaspersky Security защищает виртуальные машины.

Информация о профилях защиты 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 виртуальная машина исключена из защиты, в графе **Профиль защиты** указывается *(Нет защиты)*.

Работа с дополнительными профилями защиты

Вы можете выполнять следующие действия с профилями защиты:

- Создавать профили защиты (корневой профиль защиты формируется во время создания политики).
- Назначать виртуальным машинам профили защиты.
- Изменять параметры профилей защиты.
- Экспортировать параметры профиля защиты в файл и использовать ранее сохраненные параметры при создании нового профиля защиты. Вы можете экспортировать параметры созданных вами профилей защиты, параметры корневого профиля защиты экспортировать нельзя.
- Удалять профили защиты (корневой профиль защиты недоступен для удаления).

В этом разделе

Создание профиля защиты

Настройка 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. 194).

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, в политике которого вы хотите создать профиль защиты.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
5. В окне свойств политики выберите раздел **Профили защиты**.

   В правой части окна отобразится список профилей защиты. Если вы создаете первый профиль защиты в этой политике, то список профилей защиты пуст.
6. Нажмите на кнопку **Добавить**.

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

Имя профиля защиты не может содержать более 255 символов.

8. Если вы хотите при создании нового профиля защиты использовать ранее сохраненные параметры профиля защиты (см. раздел "Экспорт параметров профиля защиты" на стр. 123), установите флажок **Импортировать параметры из файла** и укажите путь к файлу в формате JSON.

9. 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.

   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**.

   Остальные параметры профиля защиты аналогичны параметрам корневого профиля защиты (см. раздел "Параметры корневого профиля защиты" на стр. 104).

10. После настройки всех параметров профиля защиты нажмите на кнопку **ОК** в окне **Параметры защиты**.

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

После того как вы создали профиль защиты, вы можете назначить его виртуальным машинам (см. раздел "Назначение виртуальной машине профиля защиты" на стр. 120).

Назначение виртуальной машине профиля защиты

После создания политики всем объектам управления VMware назначается корневой профиль защиты (см. раздел "О политике Kaspersky Security и профилях защиты" на стр. 94). Вы можете назначить виртуальным машинам собственный профиль защиты.

► *Чтобы назначить виртуальной машине профиль защиты, выполните следующие действия:*

1. Откройте для просмотра защищаемую инфраструктуру кластера KSC, в составе которой находится нужная вам виртуальная машина (см. раздел "Просмотр защищаемой инфраструктуры кластера KSC" на стр. 113).

2. Выполните одно из следующих действий:

   - Если вы хотите назначить профиль защиты одной виртуальной машине, выберите ее в таблице.

   - Если вы хотите назначить одинаковый профиль защиты нескольким виртуальным машинам, которые являются дочерними объектами одного объекта управления VMware, выберите в таблице этот объект управления VMware. Вы можете выбрать несколько объектов управления VMware одновременно, удерживая клавишу **CTRL**.

3. Нажмите на кнопку **Назначить профиль защиты**.

   Откроется окно **Назначенный профиль защиты**.

4. В окне **Назначенный профиль защиты** выберите один из следующих вариантов:

   - **Родительский "N"**, где N – название профиля защиты, назначенного родительскому объекту. Виртуальной машине назначается профиль защиты родительского объекта.

   - **Указанный**. Виртуальной машине назначается профиль защиты, выбранный в раскрывающемся списке из числа существующих в политике.

5. Если у выбранного объекта управления VMware есть дочерние объекты, профиль защиты назначается объекту управления VMware и всем его дочерним объектам, включая объекты, которым назначен собственный профиль защиты или которые исключены из защиты. Если вы хотите назначить профиль защиты только объекту управления VMware и тем его дочерним объектам, которым не назначен собственный профиль защиты и которые не исключены из защиты, снимите флажок **Назначить выбранный профиль всем дочерним объектам**.

6. Нажмите на кнопку **ОК**.

   Назначенный профиль защиты отобразится в таблице в графе **Профиль защиты**.

Изменение параметров профиля защиты

Вы можете изменить как параметры созданного вами профиля защиты, так и параметры корневого профиля защиты.

Настройка 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. 194).

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

► *Чтобы изменить параметры профиля защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, в политике которого вы хотите изменить профиль защиты.

3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
5. Если вы хотите изменить параметры корневого профиля защиты, выполните следующие действия:
   a. В окне **Свойства: <Название политики>** выберите раздел **Корневой профиль защиты**.
   b. В правой части окна измените параметры корневого профиля защиты (на стр. 104).
   c. Нажмите на кнопку **ОК**.
6. Если вы хотите изменить параметры созданного вами профиля защиты, выполните следующие действия:
   a. В окне **Свойства: <Название политики>** выберите раздел **Профили защиты**.

      В правой части окна отобразится список профилей защиты.
   b. В списке профилей защиты выберите профиль защиты, параметры которого вы хотите изменить, и нажмите на кнопку **Изменить**.

      Откроется окно **Параметры защиты**.
   c. Измените параметры профиля защиты (см. раздел "Создание профиля защиты" на стр. 118).
   d. Нажмите на кнопку **ОК** в окне **Параметры защиты**.
7. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

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

Экспорт параметров профиля защиты

► *Чтобы экспортировать в файл параметры профиля защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, в политике которого находится нужный вам профиль защиты.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
5. В окне свойств политики выберите раздел **Профили защиты**.

   В правой части окна отобразится список профилей защиты.
6. Выберите профиль защиты, параметры которого вы хотите экспортировать в файл, и нажмите на кнопку **Экспорт**. В открывшемся окне укажите путь к файлу в формате JSON.
7. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Ранее сохраненные параметры профиля защиты вы можете использовать при создании нового профиля защиты (см. раздел "Создание профиля защиты" на стр. 118).

Удаление профиля защиты

► *Чтобы удалить профиль защиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, в политике которого вы хотите удалить профиль защиты.
3. В рабочей области выберите закладку **Политики**.

4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.

5. В окне **Свойства: <Название политики>** выберите раздел **Профили защиты**.

   В правой части окна отобразится список профилей защиты.

6. В списке профилей защиты выберите профиль защиты, который вы хотите удалить, и нажмите на кнопку **Удалить**.

7. Если этот профиль защиты назначен виртуальным машинам, откроется окно подтверждения удаления. Нажмите на кнопку **Да**.

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

Профиль защиты будет удален. Программа будет защищать те виртуальные машины, для которых ранее использовался этот профиль защиты, с параметрами профиля защиты их родительского объекта в виртуальной инфраструктуре. Если родительский объект исключен из защиты, программа не будет защищать эти виртуальные машины.

Выключение защиты на виртуальной машине

Выключение функции защиты приводит к выходу программы из сертифицированного состояния.

► *Чтобы выключить защиту на виртуальной машине, выполните следующие действия:*

1. Откройте для просмотра защищаемую инфраструктуру кластера KSC, в составе которой находится нужная вам виртуальная машина.

2. Выполните одно из следующих действий:

   - Если вы хотите выключить защиту на одной виртуальной машине, выберите ее в таблице.

- Если вы хотите выключить защиту на нескольких виртуальных машинах, которые являются дочерними объектами одного объекта управления VMware, выберите в таблице этот объект управления VMware.

  Вы можете выбрать несколько объектов управления VMware одновременно, удерживая клавишу **CTRL**.

3. Нажмите на кнопку **Снять защиту**.

4. Если вы выбрали объект управления VMware, дочерним объектам которого назначены собственные профили защиты, откроется окно с запросом о снятии защиты с дочерних объектов. Выполните одно из следующих действий:

   - Нажмите на кнопку **Да**, если вы хотите снять защиту со всех дочерних объектов, включая объекты, которым назначен собственный профиль защиты.

   - Нажмите на кнопку **Нет**, если вы хотите оставить под защитой программы дочерние объекты, которым назначен собственный профиль защиты. Защита будет снята с родительского объекта и тех его дочерних объектов, у которых профиль защиты унаследован от родительского объекта.

   У объектов, которые исключены из защиты, в графе **Профиль защиты** отображается надпись *(Нет защиты)*.

Файловый Антивирус. Проверка виртуальных машин

Kaspersky Security позволяет проверять файлы виртуальных машин на наличие в них вирусов и других программ, представляющих угрозу. Требуется периодически проверять файлы виртуальных машин с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов.

Kaspersky Security проверяет виртуальные машины, которые соответствуют следующим требованиям:

- В инфраструктуре под управлением сервера VMware vCenter и VMware NSX Manager:
  - Виртуальная машина с операционной системой Windows включена и на ней установлен и включен драйвер VMware NSX File Introspection.
  - Виртуальная машина с операционной системой Linux включена и на ней установлен и включен драйвер VMware Linux Thin Agent.

    > Kaspersky Security проверяет виртуальные машины с операционными системами Linux, только если вы используете платформу VMware NSX for vSphere версии 6.3.1.

  - Для включенных виртуальных машин: виртуальная машина входит в состав группы безопасности NSX (NSX Security Group), настроенной в консоли VMware vSphere Web Client. Для этой группы назначена политика безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

    Выключенные виртуальные машины с файловой системой NTFS или FAT32 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).

- В инфраструктуре под управлением сервера VMware vCenter и VMware vShield Manager: виртуальная машина включена и на ней установлен и включен драйвер VMware NSX File Introspection.

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

Если во время проверки файлов виртуальных машин 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*.

При проверке виртуальных машин используются сигнатурный и эвристический анализ. При *сигнатурном анализе* используются базы Kaspersky Security, содержащие информацию об известных угрозах и о методах их устранения. Проверка с использованием сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

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.

Kaspersky Security использует для проверки следующие задачи:

- **Полная проверка**. В процессе выполнения задачи SVM проверяют на вирусы и другие программы, представляющие угрозу, все виртуальные машины в составе защищаемой инфраструктуры указанного кластера KSC или всех кластеров KSC, входящих в указанную группу администрирования.

- **Выборочная проверка**. В процессе выполнения задачи SVM проверяют на вирусы и другие программы, представляющие угрозу, выбранные виртуальные машины в составе защищаемой инфраструктуры указанного кластера KSC. Задача выборочной проверки позволяет проверять виртуальные машины, находящиеся под управлением одного сервера VMware vCenter.

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 файловой системой NTFS или FAT32.

- 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 другой 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, если директории, в которые смонтированы сетевые файловые системы, входят в область проверки задачи.

- Во время выполнения задачи проверки одна SVM с установленным компонентом Файловый Антивирус одновременно проверяет файлы не более четырех виртуальных машин.

Kaspersky Security 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.

Вы можете запускать задачу проверки вручную или задать расписание выполнения задачи проверки.

Процесс выполнения проверки отображается на закладке **Задачи** рабочей области папки с названием кластера KSC, для SVM которого вы запустили задачу проверки.

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 на виртуальной машине" на стр. 124). 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. Откройте Консоль администрирования Kaspersky Security Center.
2. 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.
3. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

В этом разделе

Шаг 1. Выбор типа задачи

На этом шаге для программы **Kaspersky Security для виртуальных сред 4.0 Защита без агента** в качестве типа задачи выберите **Полная проверка**.

Перейдите к следующему шагу мастера создания задачи.

Шаг 2. Настройка параметров проверки

На этом шаге укажите параметры проверки виртуальных машин.

Настройка 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. 194).

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

► *Чтобы указать параметры проверки виртуальных машин, выполните следующие действия:*

1. 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**

        Удаление 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**.

  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**

  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 компьютере пользователя. 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 других легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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 или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нанесения вреда компьютеру или данным пользователя.

  Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы:

   - **Выбирать действие автоматически**

     Kaspersky Security выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию. Это действие **Лечить. Удалять, если лечение невозможно**.

     Этот вариант действия выбран по умолчанию.

- **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 установлен флажок **Удалять архивы, если лечение не удалось** в параметрах уровня безопасности.

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

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

- **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. Kaspersky Security может проверять выключенные виртуальные машины с операционными системами Windows или Linux и файловой системой NTFS или FAT32. Если вы хотите, чтобы программа проверяла выключенные виртуальные машины, установите флажок **Проверять выключенные виртуальные машины** в блоке **Дополнительные параметры проверки**.

   Kaspersky Security не проверяет файлы на выключенных виртуальных машинах с другими файловыми системами.

   > Во время проверки выключенную виртуальную машину невозможно включить или выполнить ее миграцию.

4. При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security может проверять файлы на оптических дисках (CD, DVD, Blu-Ray). Если вы хотите, чтобы программа проверяла файлы на оптических дисках, установите флажок **Проверять оптические диски** в блоке **Дополнительные параметры проверки**.

   > Если флажок **Проверять оптические диски** установлен, но в область проверки для задачи не включен путь к оптическому диску, Kaspersky Security не проверяет оптический диск.

   Kaspersky Security не проверяет файлы на оптических дисках при проверке выключенных виртуальных машин и виртуальных машин с операционными системами Linux.

5. 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.

     По умолчанию выбран этот вариант.

     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 полной проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах.

     Задача выборочной проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах, входящих в область действия задачи.

Перейдите к следующему шагу мастера создания задачи.

Шаг 3. Выбор области проверки

На этом шаге требуется сформировать область проверки задачи. Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Настройка 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. 194).

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

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 другой 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, если директории, в которые смонтированы сетевые файловые системы, входят в область проверки задачи.

Выберите один из следующих вариантов:

- **Проверять все папки и файлы, кроме указанных**.
- **Проверять только указанные папки и файлы**.

Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список объектов, которые требуется исключить из области проверки. 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.

  > Если вы указали путь к папке и установили флажок **Применять к вложенным**, из области проверки будут исключены все папки, которые находятся по указанному пути и имя которых начинается с указанного имени. Например, если вы указали путь к папке в виде "C:\temp", то папка, расположенная по пути "C:\temp-2", тоже будет исключена из области проверки.

- 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**.

> В списке исключений не поддерживается использование переменных окружения. Объект файловой системы, заданный с использованием переменных окружения, не исключается из области проверки. Если вы импортировали список исключений, который содержит переменные окружения, вам требуется заменить переменные окружения абсолютными значениями.

В блоке **Расширения файлов** укажите расширения файлов, которые вы хотите 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 защиты.
- **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. При указании расширений файлов вы можете использовать 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.

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 надо 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.

Перейдите к следующему шагу мастера создания задачи.

Шаг 4. Выбор SVM

Этот шаг доступен, если вы запустили мастер создания задачи из папки **Задачи**.

Укажите способ выбора SVM, для которых вы создаете задачу:

- Нажмите на кнопку **Выбрать устройства, обнаруженные в сети Сервером администрирования**, если вы хотите выбрать SVM из списка виртуальных машин, 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 вы хотите создать задачу для выборки SVM по предопределенному критерию. О создании выборки устройств см. 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, для которых вы создаете задачу. Для этого установите флажок в списке слева от названия 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, для которых вы создаете задачу.

Перейдите к следующему шагу мастера создания задачи.

Шаг 5. Определение параметров расписания запуска задачи

На этом шаге настройте режим запуска задачи:

- **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.

- **Автоматически определять интервал для распределения запуска 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 **Автоматически определять интервал для распределения запуска задачи**. По умолчанию флажок установлен.

- **Распределять запуск задачи случайным образом 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 **Автоматически определять интервал для распределения запуска задачи**.

Распределенный запуск задачи помогает избежать одновременного обращения большого количества SVM к Серверу администрирования Kaspersky Security Center.

Перейдите к следующему шагу мастера создания задачи.

Шаг 6. Определение названия задачи

На этом шаге в поле **Имя** введите имя задачи.

Перейдите к следующему шагу мастера создания задачи.

Шаг 7. Завершение создания задачи

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 проверки отобразится в списке задач.

Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска задачи, то задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить или остановить задачу вручную (см. раздел "Запуск, остановка и просмотр результатов запуска задач" на стр. 98).

Создание задачи выборочной проверки

В случае замены / переустановки сервера VMware vCenter 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 в свойствах этой задачи.

► *Чтобы создать задачу выборочной проверки, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите папку с название кластера KSC, для SVM которого вы хотите создать задачу выборочной проверки.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**, чтобы запустить мастер создания задачи.
5. Следуйте указаниям мастера создания задачи.

В этом разделе

Шаг 1. Выбор типа задачи

На этом шаге для программы **Kaspersky Security для виртуальных сред 4.0 Защита без агента** в качестве типа задачи выберите **Выборочная проверка**.

Перейдите к следующему шагу мастера создания задачи.

Шаг 2. Подключение к Серверу интеграции

Укажите параметры подключения 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, вы можете использовать вашу доменную учетную запись для подключения к Серверу интеграции. 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 сохраненный пароль администратора отображается в окне ввода параметров подключения.

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. 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, в разделе HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<адрес>\, где <адрес> – адрес Сервера интеграции, от которого получен сертификат. 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.

Откроется окно **Список серверов VMware vCenter**. Выберите сервер VMware vCenter, соответствующий кластеру KSC, для SVM которого вы хотите создать задачу выборочной проверки, и нажмите на кнопку **ОК**.

Шаг 3. Выбор области действия задачи

На этом шаге укажите виртуальные машины, файлы которых вы хотите проверить.

Виртуальная инфраструктура VMware под управлением одного сервера VMware vCenter отображается в таблице в виде дерева объектов: сервер VMware vCenter, 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.

> 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.

Шаг 4. Настройка параметров проверки

На этом шаге укажите параметры проверки виртуальных машин.

Настройка 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. 194).

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

► *Чтобы указать параметры проверки виртуальных машин, выполните следующие действия:*

1. 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**

  Удаление 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**.

  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**

  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 компьютере

пользователя. 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 других легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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 или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нанесения вреда компьютеру или данным пользователя.

Если флажок установлен, защита от легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру 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, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы:

- **Выбирать действие автоматически**

  Kaspersky Security выполняет действие, заданное специалистами "Лаборатории Касперского" по умолчанию. Это действие **Лечить. Удалять, если лечение невозможно**.

  Этот вариант действия выбран по умолчанию.

- **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 установлен флажок **Удалять архивы, если лечение не удалось** в параметрах уровня безопасности.

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

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

- **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. Kaspersky Security может проверять выключенные виртуальные машины с операционными системами Windows или Linux и файловой системой NTFS или FAT32. Если вы хотите, чтобы программа проверяла выключенные виртуальные машины, установите флажок **Проверять выключенные виртуальные машины** в блоке **Дополнительные параметры проверки**.

   Kaspersky Security не проверяет файлы на выключенных виртуальных машинах с другими файловыми системами.

   > Во время проверки выключенную виртуальную машину невозможно включить или выполнить ее миграцию.

4. При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security может проверять файлы на оптических дисках (CD, DVD, Blu-Ray). Если вы хотите, чтобы программа проверяла файлы на оптических дисках, установите флажок **Проверять оптические диски** в блоке **Дополнительные параметры проверки**.

   > Если флажок **Проверять оптические диски** установлен, но в область проверки для задачи не включен путь к оптическому диску, Kaspersky Security не проверяет оптический диск.

   Kaspersky Security не проверяет файлы на оптических дисках при проверке выключенных виртуальных машин и виртуальных машин с операционными системами Linux.

5. 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.

По умолчанию выбран этот вариант.

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 полной проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах.

  Задача выборочной проверки выполняется до тех пор, пока не будет завершена проверка файлов на всех защищенных виртуальных машинах, входящих в область действия задачи.

Перейдите к следующему шагу мастера создания задачи.

Шаг 5. Выбор области проверки

На этом шаге требуется сформировать область проверки задачи. Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Настройка 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. 194).

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

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 другой 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, если директории, в которые смонтированы сетевые файловые системы, входят в область проверки задачи.

Выберите один из следующих вариантов:

- **Проверять все папки и файлы, кроме указанных**.
- **Проверять только указанные папки и файлы**.

Если вы выбрали вариант **Проверять все папки и файлы, кроме указанных**, с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список объектов, которые требуется исключить из области проверки. 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.

  Если вы указали путь к папке и установили флажок **Применять к вложенным**, из области проверки будут исключены все папки, которые находятся по указанному пути и имя которых начинается с указанного имени. Например, если вы указали путь к папке в виде "C:\temp", то папка, расположенная по пути "C:\temp-2", тоже будет исключена из области проверки.

- 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**.

В списке исключений не поддерживается использование переменных окружения. Объект файловой системы, заданный с использованием переменных окружения, не исключается из области проверки. Если вы импортировали список исключений, который содержит переменные окружения, вам требуется заменить переменные окружения абсолютными значениями.

В блоке **Расширения файлов** укажите расширения файлов, которые вы хотите 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 защиты.

- **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. При указании расширений файлов вы можете использовать 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.

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 надо 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.

Перейдите к следующему шагу мастера создания задачи.

Шаг 6. Определение параметров расписания запуска задачи

На этом шаге настройте режим запуска задачи:

- **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.

- **Автоматически определять интервал для распределения запуска 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 **Автоматически определять интервал для распределения запуска задачи**. По умолчанию флажок установлен.

- **Распределять запуск задачи случайным образом 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 **Автоматически определять интервал для распределения запуска задачи**.

  Распределенный запуск задачи помогает избежать одновременного обращения большого количества SVM к Серверу администрирования Kaspersky Security Center.

Перейдите к следующему шагу мастера создания задачи.

Шаг 7. Определение названия задачи

На этом шаге в поле **Имя** введите имя задачи.

Перейдите к следующему шагу мастера создания задачи.

Шаг 8. Завершение создания задачи

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 проверки отобразится в списке задач.

Если в окне **Настройка расписания запуска задачи** вы задали расписание запуска задачи, то задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить или остановить задачу вручную (см. раздел "Запуск, остановка и просмотр результатов запуска задач" на стр. 98).

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 Файловый Антивирус. 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. 163).

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 Файловый Антивирус.

В этом разделе

Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для SVM которого вы хотите настроить параметры резервного хранилища.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику, настроенную для SVM этого кластера KSC, и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
5. В окне свойств политики выберите раздел **Резервное хранилище**.
6. 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.

7. Нажмите на кнопку **ОК**.

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, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли 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.

Обновление баз программы

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. 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 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. Подробнее см. в документации 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.

  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.

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. Если задача загрузки обновлений в хранилище отсутствует, создайте ее (см. в документации Kaspersky Security Center).

2. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы. 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 **Создать задачу**, чтобы запустить мастер создания задачи.

c. На первом шаге мастера выберите для программы **Kaspersky Security для виртуальных сред 4.0 Защита без агента** в качестве типа задачи **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 виртуальных машин укажите SVM, для которых вы создаете задачу. 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, для которых вы создаете задачу.

   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 "Запуск, остановка и просмотр результатов запуска задач" на стр. 98).

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 для всех SVM, для SVM одного кластера KSC или для отдельной SVM 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 **Создать задачу**, чтобы запустить мастер создания задачи.

   c. На первом шаге мастера выберите для программы **Kaspersky Security для виртуальных сред 4.0 Защита без агента** в качестве типа задачи **Откат обновления**. 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 виртуальных машин укажите SVM, для которых вы создаете задачу. 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, для которых вы создаете задачу.

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 "Запуск, остановка и просмотр результатов запуска задач" на стр. 98).

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.

В зависимости от расположения инфраструктуры KSN различают:

- Глобальный KSN – инфраструктура расположена на серверах "Лаборатории Касперского".
- Локальный KSN (Kaspersky Private Security Network) – инфраструктура расположена на сторонних серверах поставщика услуг, например внутри сети интернет-провайдера.

Информация о том, какой тип KSN использует программа Kaspersky Security, отображается в свойствах политики (см. раздел "Настройка использования Kaspersky Security Network" на стр. 176).

Использование Глобального KSN приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Локальный KSN.

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

Если вы участвуете в Kaspersky Security Network и используете Глобальный KSN, определенная информация, полученная в результате работы Kaspersky Security, автоматически отправляется в "Лабораторию Касперского" (см. раздел "О предоставлении данных" на стр. 175).

Взаимодействие между инфраструктурой KSN и SVM, находящимися под управлением Kaspersky Security Center, обеспечивает служба *KSN Proxy*. Настройка службы KSN Proxy выполняется в свойствах Сервера администрирования Kaspersky Security Center.

Если служба KSN Proxy отключена в Kaspersky Security Center, обмен данными между SVM и Kaspersky Security Network не производится. Если при этом использование KSN включено в политике Kaspersky Security, возможно снижение производительности работы программы Kaspersky Security. Рекомендуется отключить использование KSN в политике Kaspersky Security, если служба KSN Proxy отключена в Kaspersky Security Center.

Подробнее о службе KSN Proxy см. в документации Kaspersky Security Center.

Ваше участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний Kaspersky Security.

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 (см. раздел "Настройка использования Kaspersky Security Network" на стр. 176).

В этом разделе

О предоставлении данных

Если вы участвуете в Kaspersky Security Network и используете Глобальный KSN, вы соглашаетесь передавать в «Лабораторию Касперского» в автоматическом режиме следующие сведения:

- номер версии и тип программы;
- название и версию операционной системы, установленной на SVM с установленным компонентом Файловый Антивирус, и установленные пакеты обновлений для операционной системы;
- IP-адрес SVM с установленным компонентом Файловый Антивирус;
- версию операционной системы защищенной виртуальной машины, на которой проверялся файл;
- тип и срок действия лицензии, ключ или код активации, идентификатор партнера, у которого приобретена лицензия;
- уникальный идентификатор установки программы (уникальный идентификатор из BIOS SVM с установленным компонентом Файловый Антивирус);
- MD5-хеш файла;
- информацию об обнаруженных зараженных файлах (имя зараженного файла, размер распакованного файла в байтах, полный путь к файлу, статус файла, код типа файла, идентификатор типа файла, название обнаруженного объекта, дата и время выпуска баз программы, версия баз программы, тип, идентификатор и версия записи баз программы, идентификатор типа задачи обновления баз);
- количество неудачных попыток обновления баз программы (если задача обновления завершена с ошибкой);
- результат обновления баз программы.

Для проверки в «Лабораторию Касперского» могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда виртуальной машине или хранящимся в ее операционной системе данным.

Если вы не участвуете в программе Kaspersky Security Network, перечисленные выше данные не передаются. Данные обрабатываются и хранятся в ограниченном и защищенном разделе на виртуальной машине. Указанные данные безвозвратно удаляются при удалении программы.

О данных, которые Kaspersky Security передает в Kaspersky Security Network, вы можете также прочитать в Положении о Kaspersky Security Network перед принятием решения об участии в KSN.

Информация о том, как происходит обработка данных, описана на веб-сайте "Лаборатории Касперского" (http://www.kaspersky.ru/privacy).

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

Настройка использования Kaspersky Security Network

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

Настройка использования Kaspersky Security Network выполняется в параметрах политики. Если в активной политике кластера KSC использование KSN включено, службы KSN

используются в работе Kaspersky Security как во время защиты виртуальных машин, так и при выполнении задач проверки виртуальных машин.

Если политика, в которой использование KSN включено, не активна, службы KSN не используются в работе программы Kaspersky Security.

Если вы хотите использовать Kaspersky Security Network в работе Kaspersky Security, убедитесь в том, что служба KSN Proxy включена в Kaspersky Security Center (см. в документации Kaspersky Security Center).

► *Чтобы настроить использование Kaspersky Security Network, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для SVM которого вы хотите настроить использование Kaspersky Security Network.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно **Свойства: <Название политики>**.
5. В окне свойств политики выберите раздел **Параметры KSN**.
6. Настройте следующие параметры:

   - **Я принимаю условия участия в программе Kaspersky Security Network**

     Включение / выключение использования Глобального KSN в работе Kaspersky Security.

     Если флажок установлен и в свойствах Сервера администрирования Kaspersky Security Center не настроено использование Локального KSN, в работе программы используется Глобальный KSN.

     Если флажок снят, Глобальный KSN в работе программы не используется.

     По умолчанию флажок снят.

Условия участия в программе Kaspersky Security Network изложены в Положении о Kaspersky Security Network.

- **Использовать Локальный KSN, если он настроен в Kaspersky Security Center**

  Включение / выключение использования Локального KSN в работе Kaspersky Security.

  Если использование Локального KSN не настроено в Kaspersky Security Center, использовать Локальный KSN в работе программы невозможно. Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

  Если флажок установлен и в свойствах Сервера администрирования Kaspersky Security Center настроено использование Локального KSN, в работе программы используется Локальный KSN.

  Если флажок снят, Локальный KSN не используется.

  Флажок установлен в то положение, которое вы выбрали при создании политики.

7. Нажмите на кнопку **ОК**.

События

SVM отправляют на Сервер администрирования Kaspersky Security Center служебные сообщения с информацией о работе Kaspersky Security – *события*.

Выделяют следующие уровни важности событий:

- **Критическое событие**. События критической важности, в том числе указывающие на проблемы в работе Kaspersky Security или на уязвимости в защите виртуальных машин.
- **Отказ функционирования**. События об отказе функционирования программы.
- **Предупреждение**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Security.
- **Информационное сообщение**. События справочного характера.

Kaspersky Security передает на Сервер администрирования Kaspersky Security Center следующие данные о виртуальных машинах:

- имя виртуальной машины и путь к ней в виртуальной инфраструктуре;
- состояние защиты виртуальной машины;
- профиль защиты;
- дату последней проверки виртуальной машины;
- полные пути к файлам, пропущенным программой при проверке или классифицированным программой как зараженные.

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. 180).

Уведомление – это сообщение с информацией о событии, которое произошло на SVM. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе программы.

Вы можете настроить параметры событий Kaspersky Security в политике (см. раздел "Настройка параметров событий Kaspersky Security" на стр. 181).

Подробную информацию о событиях и уведомлениях см. в документации Kaspersky Security Center.

> В событиях Kaspersky Security Center в качестве названия виртуальной машины может отображаться имя виртуальной машины и путь к ней в виртуальной инфраструктуре.

В этом разделе

Просмотр событий

► *Чтобы посмотреть список всех событий в работе Сервера администрирования Kaspersky Security Center, управляемых устройств и программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В рабочей области узла **Сервер администрирования** перейдите на закладку **События**.

В списке отображаются события из выборки, которая в настоящий момент указана в раскрывающемся списке **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 событий Kaspersky Security

Настройка 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. 194).

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

► *Чтобы настроить параметры событий Kaspersky Security, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли выберите группу администрирования, содержащую кластер KSC, для SVM которого вы хотите настроить параметры событий.
3. В рабочей области выберите закладку **Политики**.
4. В списке политик выберите политику и откройте окно свойств политики одним из следующих способов:
   - Двойным щелчком мыши.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название политики>**.
5. В окне свойств политики выберите раздел **Оповещение о событиях**.
6. Выберите закладку с названием уровня важности событий, параметры которых вы хотите настроить:
   - **Критическое событие**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.
7. Выберите типы событий, параметры которых вы хотите настроить:
   - Используйте клавиши **SHIFT** и **CTRL**, если вы хотите выбрать несколько типов событий.
   - Нажмите на кнопку **Выбрать все**, если вы хотите выбрать все типы событий.
8. Нажмите на кнопку **Свойства**.

9. Откроется окно **Свойства <N событий>**, где N – количество выбранных типов событий.

10. 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.

11. В блоке **Уведомления о событиях** выберите способ уведомления:

    - **Уведомлять по электронной почте**.
    - **Уведомлять по SMS**.
    - **Уведомлять запуском исполняемого файла или скрипта**.
    - **Уведомлять по SNMP**.

12. Нажмите на кнопку **ОК** в окне **Свойства <N событий>**.

13. Нажмите на кнопку **ОК**.

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.
- На форуме "Лаборатории Касперского" (http://forum.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 186).

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 (http://support.kaspersky.ru/support/rules).

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 (http://support.kaspersky.ru/support/rules).

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 (http://support.kaspersky.ru/faq/companyaccount_help).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	http://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Mac – товарный знак Apple Inc., зарегистрированный в США и других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Excel, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat Enterprise Linux – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware, VMware ESXi, VMware NSX Manager, VMware NSX for vSphere, VMware vCenter, VMware vCloud Networking and Security, VMware vShield, VMware vShield Endpoint, VMware vShield Manager, VMware Tools, VMware vSphere и VMware vSphere Web Client – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 2. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

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
Корневой профиль защиты	**Включить защиту**	Флажок установлен.
Корневой профиль защиты, дополнительный профиль защиты, задача полной проверки, задача выборочной проверки	**Действие при обнаружении угрозы**	Одно из следующих значений: **- Выбирать действие автоматически**. **- Лечить. Удалять, если лечение невозможно**. **- Лечить. Блокировать, если лечение невозможно**.
Корневой профиль защиты, дополнительный профиль защиты, задача полной проверки	**Проверять все, кроме файлов со следующими расширениями**	Пусто.
Корневой профиль защиты, дополнительный профиль защиты, задача полной проверки	**Проверять только файлы со следующими расширениями**	Пусто.
Корневой профиль защиты	**Папки и файлы**	Пусто или только заданный по умолчанию список исключений, рекомендуемых корпорацией Microsoft.
Дополнительный профиль защиты, задача полной проверки	**Папки и файлы**	Пусто.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Параметры SNMP-мониторинга в политике	**Включить SNMP-мониторинг состояния SVM**	Флажок снят.
Параметры использования KSN в политике	**Я принимаю условия участия в программе Kaspersky Security Network**	Флажок снят.
Параметры событий Kaspersky Security в политике	**На Сервере администрирования в течение (сут)**	Флажок установлен, значение не ниже заданного по умолчанию.
Корневой профиль защиты, дополнительный профиль защиты	**Проверять сетевые диски**	Флажок установлен при наличии сетевых дисков на защищаемой виртуальной машине. Если сетевые диски отсутствуют, флажок может быть снят.
Защищаемая инфраструктура в политике	**Профиль защиты**	Одно из следующих значений: - **унаследованный: <N>**, где N – название унаследованного от родительского объекта профиля защиты; - **<N>**, где N – название назначенного профиля защиты, в том числе **Корневой**.

Сущность, к которой относится параметр	Название параметра	Значение параметра в сертифицированном состоянии программы
Задача полной проверки	**Проверять оптические диски**	Флажок установлен при наличии оптического привода на защищаемой виртуальной машине. Если оптический привод отсутствует, флажок может быть снят.
Задача обновления баз программы	**Запуск по расписанию**	**При загрузке обновлений в хранилище**.