Содержание

Об этой справке

Эта справка адресована техническим специалистам, в обязанности которых входит администрирование Kaspersky Security, а также поддержка организаций, использующих Kaspersky Security. Руководство адресовано техническим специалистам, которые имеют опыт работы с виртуальной инфраструктурой на платформе VMware vSphere и системой удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center.

О Kaspersky Kaspersky Security для виртуальных и облачных сред

Kaspersky Kaspersky Security для виртуальных и облачных сред (далее также "Kaspersky Security") представляет собой интегрированное решение, обеспечивающее защиту виртуальных машин на гипервизоре VMware ESXi от вирусов и других вредоносных программ, а также от сетевых угроз.

Kaspersky Security позволяет защищать виртуальные машины с гостевыми операционными системами Windows, в том числе и с операционными системами для серверов, а также виртуальные машины с гостевыми операционными системами Linux.

Kaspersky Security позволяет настраивать защиту виртуальных машин на любом уровне иерархии объектов виртуальной инфраструктуры VMware: сервер VMware vCenter Server, объект Datacenter, кластер VMware, ресурсный пул, объект vApp, виртуальная машина. Программа поддерживает защиту виртуальных машин во время их миграции в рамках DRS-кластера VMware.

В инфраструктуре под управлением сервера VMware vCloud Director программа Kaspersky Security может использоваться для защиты изолированных виртуальных инфраструктур – виртуальных Datacenter, соответствующих организациям vCloud Director. Один экземпляр программы Kaspersky Security в режиме multitenancy позволяет нескольким арендаторам облачной инфраструктуры (организациям-клиентам или подразделениям одной организации) независимо управлять защитой своей виртуальной инфраструктуры.

В состав Kaspersky Security входят следующие компоненты:

- Защита от файловых угроз. Компонент позволяет избежать заражения объектов файловой системы виртуальной машины. Компонент запускается при старте Kaspersky Security и выполняет функции защиты виртуальных машин и проверки объектов файловой системы виртуальных машин.

- Защита от сетевых угроз. Компонент позволяет обнаруживать и блокировать активность, характерную для сетевых атак, и другую подозрительную сетевую активность, а также проверять веб-адреса, к которым обращается пользователь или какая-либо программа, и блокировать доступ к веб-адресам в случае обнаружения угрозы.

- Сервер интеграции. Компонент осуществляет взаимодействие между компонентами программы Kaspersky Security и виртуальной инфраструктурой VMware.

Kaspersky Security предоставляет следующие возможности:

- Защита. Kaspersky Security проверяет все файлы, которые пользователь или какая-либо программа открывает, сохраняет или запускает на виртуальной машине.

  - Если в файле не обнаружены вредоносные программы, программа Kaspersky Security разрешает доступ к этому файлу.

  - Если в файле обнаружены вредоносные программы, программа Kaspersky Security выполняет то действие, которое указано в ее параметрах, например удаляет файл или блокирует доступ к файлу.

  Kaspersky Security защищает только включенные виртуальные машины, для которых выполняются все условия защиты виртуальных машин.

- Проверка. Программа позволяет выполнять антивирусную проверку файлов виртуальных машин. Требуется периодически проверять файлы виртуальной машины с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов. Вы можете выполнять проверку по требованию или задать расписание проверки.

  Kaspersky Security проверяет только виртуальные машины, для которых выполняются все условия проверки виртуальных машин. Kaspersky Security может проверять выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS, а также шаблоны виртуальных машин.

- Предотвращение вторжений. Kaspersky Security позволяет анализировать сетевой трафик защищенных виртуальных машин и обнаруживать сетевые атаки и подозрительную сетевую активность, которая может быть признаком вторжения в защищаемую инфраструктуру. Обнаружив попытку сетевой атаки на виртуальную машину или подозрительную сетевую активность, Kaspersky Security может прерывать соединение и блокировать трафик с IP-адреса, который является источником сетевой атаки или подозрительной сетевой активности.

- Проверка веб-адресов. Kaspersky Security позволяет проверять веб-адреса, к которым пользователь или программа, установленная на виртуальной машине, обращается по протоколу HTTP. Если Kaspersky Security устанавливает принадлежность веб-адреса к одной из категорий веб-адресов, выбранных для обнаружения, программа может блокировать доступ к этому веб-адресу. По умолчанию Kaspersky Security проверяет вебадреса на принадлежность к вредоносным, фишинговым и рекламным веб-адресам.
- Хранение резервных копий файлов. Программа позволяет хранить резервные копии тех файлов, которые были удалены или изменены в процессе лечения. Резервные копии файлов хранятся в резервном хранилище в специальном формате и не представляют опасности. Если вылеченный файл содержал информацию, которая в результате лечения стала полностью или частично недоступна, вы можете сохранить файл из его резервной копии.

- Обновление баз программы. Загрузка обновленных баз программы обеспечивает актуальность защиты виртуальной машины от вирусов и других вредоносных программ. Вы можете запускать обновление баз программы вручную или задать расписание обновления баз программы.

Управление Kaspersky Security осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center. Используя возможности Kaspersky Security Center, вы можете:

- настраивать параметры работы программы; управлять работой программы: управлять
- защитой виртуальных машин с помощью политик; управлять задачами проверки; управлять
  - лицензионными ключами для программы; обновлять базы программы; работать с
  - резервными копиями файлов в резервном хранилище; формировать отчеты о
  - событиях, которые произошли во время работы программы.
- Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время антивирусной защиты и проверки виртуальных машин, а также о событиях, произошедших во
- время защиты от вторжений и проверки веб-адресов.
-

Комплект поставки

О приобретении программы вы можете узнать на сайте "Лаборатории Касперского" (http://www.kaspersky.ru) или у компаний-партнеров.

В комплект поставки входят файлы, необходимые для установки компонентов программы, в том числе:

- файл для запуска мастера установки компонентов Kaspersky Security (плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции);
- файл для запуска мастера установки плагина управления Kaspersky Security для клиентов (этот плагин требуется, если вы используете программу в режиме multitenancy); образы SVM (виртуальной машины защиты) с установленными
- компонентами Kaspersky Security;
- MIB-файлы, которые вы можете использовать для получения сведений о состоянии SVM с помощью системы SNMP-мониторинга;
- файл с текстом Лицензионного соглашения, в котором указано, на каких условиях вы можете пользоваться программой, и Политики конфиденциальности, которая описывает обработку и передачу данных.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

Аппаратные и программные требования

Требования к компонентам Kaspersky Security Center

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

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

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

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

Для работы программы требуются следующие компоненты Kaspersky Security Center:

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

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

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

Программные требования компонента Сервер интеграции

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

- Windows Server 2019.
- Windows Server 2016.
- Windows Server 2012 R2 Datacenter / Standard / Essentials.

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

Программные требования компонента Защита от файловых угроз

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

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

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

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

  На защищаемых виртуальных машинах с операционными системами Windows должна использоваться одна из следующих файловых систем: FAT, FAT32, NTFS, ISO9660, UDF, CIFS.
- Операционные системы Linux для серверов:

- Ubuntu Server 14.04 LTS (64-разрядная).
- Red Hat Enterprise Linux Server 7 GA (64-разрядная).
- SUSE Linux Enterprise Server 12 GA (64-разрядная).
- CentOS 7 (64-разрядная).

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

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

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

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

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

Информацию об установке и обновлении компонентов VMware см. в документации к продуктам VMware.

Программные требования компонента Защита от сетевых угроз

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

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

Требования к гостевой операционной системе защищаемой виртуальной машины совпадают с требованиями, которые предъявляет компонент Защита от файловых угроз.

Для защиты виртуальных машин от сетевых угроз на виртуальных машинах требуется установить пакет VMware Tools версии 11.0.1 или open-vm-tools.

> Для функционирования компонента Защита от сетевых угроз требуется действующая лицензия NSX for vSphere Advanced или NSX for vSphere Enterprise.

Компонент Защита от сетевых угроз обеспечивает защиту виртуальных машин, на которых используется сетевой адаптер E1000 или VMXNET3.

Программные требования для работы программы в режиме multitenancy

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

Аппаратные требования

В комплект поставки программы входит несколько образов SVM (виртуальная машина защиты) с установленным компонентом Защита от файловых угроз и несколько образов SVM с установленным компонентом Защита от сетевых угроз. С помощью этих образов вы можете развернуть SVM нужной конфигурации.

В зависимости от выбранной конфигурации для SVM с компонентом Защита от файловых угроз требуется следующее минимальное количество системных ресурсов:

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

2 CPU 1 GB RAM	2	1	26
4 CPU 2 GB RAM	4	2	27
8 CPU 4 GB RAM	8	4	29

В зависимости от выбранной конфигурации для SVM с компонентом Защита от сетевых угроз требуется следующее минимальное количество системных ресурсов:

Конфигурация	Количество процессоров	Объем выделенной оперативной памяти, ГБ	Объем выделенного свободного места на диске, ГБ

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

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

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

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

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

Что нового

В Kaspersky Kaspersky Security для виртуальных и облачных сред появились следующие новые возможности:

- Реализован новый режим работы программы: режим multitenancy. В инфраструктуре под управлением сервера VMware vCloud Director программа Kaspersky Security может использоваться для защиты изолированных виртуальных инфраструктур – виртуальных Datacenter, соответствующих организациям vCloud Director. В режиме multitenancy один экземпляр программы, установленный в инфраструктуре организации-провайдера антивирусной защиты, позволяет нескольким арендаторам облачной инфраструктуры (организациям-клиентам или подразделениям одной организации) независимо управлять защитой своей виртуальной инфраструктуры.

  Для управления защитой клиентов используются виртуальные Серверы администрирования Kaspersky Security Center. Администратор провайдера создает для каждого клиента отдельный виртуальный Сервер администрирования и предоставляет администратору клиента доступ к нему. С помощью виртуального Сервера администрирования и плагина управления для клиентов администратор клиента может управлять защитой своей виртуальной инфраструктуры от файловых угроз. Управление сетевой защитой, а также обновление баз программы, активацию программы и работу с копиями файлов, помещенных в резервное хранилище, обеспечивает провайдер.

- Расширена функциональность компонента Защита от сетевых угроз:

- При проверке веб-адресов Kaspersky Security может использовать информацию о репутации интернетресурсов полученную из Глобального KSN.

- Добавлена возможность проверки веб-адресов на принадлежность к категориям рекламных веб-адресов и веб-адресов, связанных с распространением легальных программ, которые могут быть использованы для нанесения вреда виртуальной машине или данным пользователя.

- Реализована возможность просмотра списка источников сетевых угроз, заблокированных в результате работы каждой SVM с компонентом Защита от сетевых угроз. В этом списке вы можете отменить блокировку трафика с выбранных IP-адресов, не дожидаясь автоматической разблокировки.

- Расширены возможности проверки и защиты виртуальных машин:

  - В списке исключений из проверки и защиты добавлена поддержка переменных окружения. В задачах проверки и в политиках вы можете задавать пути к объектам, исключаемым из области проверки или защиты, с использованием переменных окружения Windows.

  - В задачах проверки реализована возможность настройки действия, которое выполняет Kaspersky Security при обнаружении зараженных файлов на выключенных виртуальных машинах или шаблонах виртуальных машин. Вы можете отдельно настраивать действия при обнаружении угрозы на включенных виртуальных машинах и на выключенных виртуальных машинах.

- В политике реализован новый способ назначения параметров файловой защиты объектам защищаемой инфраструктуры (только для виртуальной инфраструктуры под управлением одного сервера VMware vCenter Server). Вы можете назначать параметры файловой защиты путем установки соответствия профилей защиты с конфигурациями профилей NSX (NSX Profile Configurations).

- Реализована возможность использовать сетевое хранилище данных для хранения резервных копий файлов, помещенных в резервные хранилища на SVM. Чтобы избежать удаления резервных копий файлов в результате удаления или обновления SVM, вы можете настроить использование сетевого хранилища данных для SVM. Если использование сетевого хранилища данных включено, резервные копии файлов сохраняются как на SVM, так и в сетевом хранилище данных.

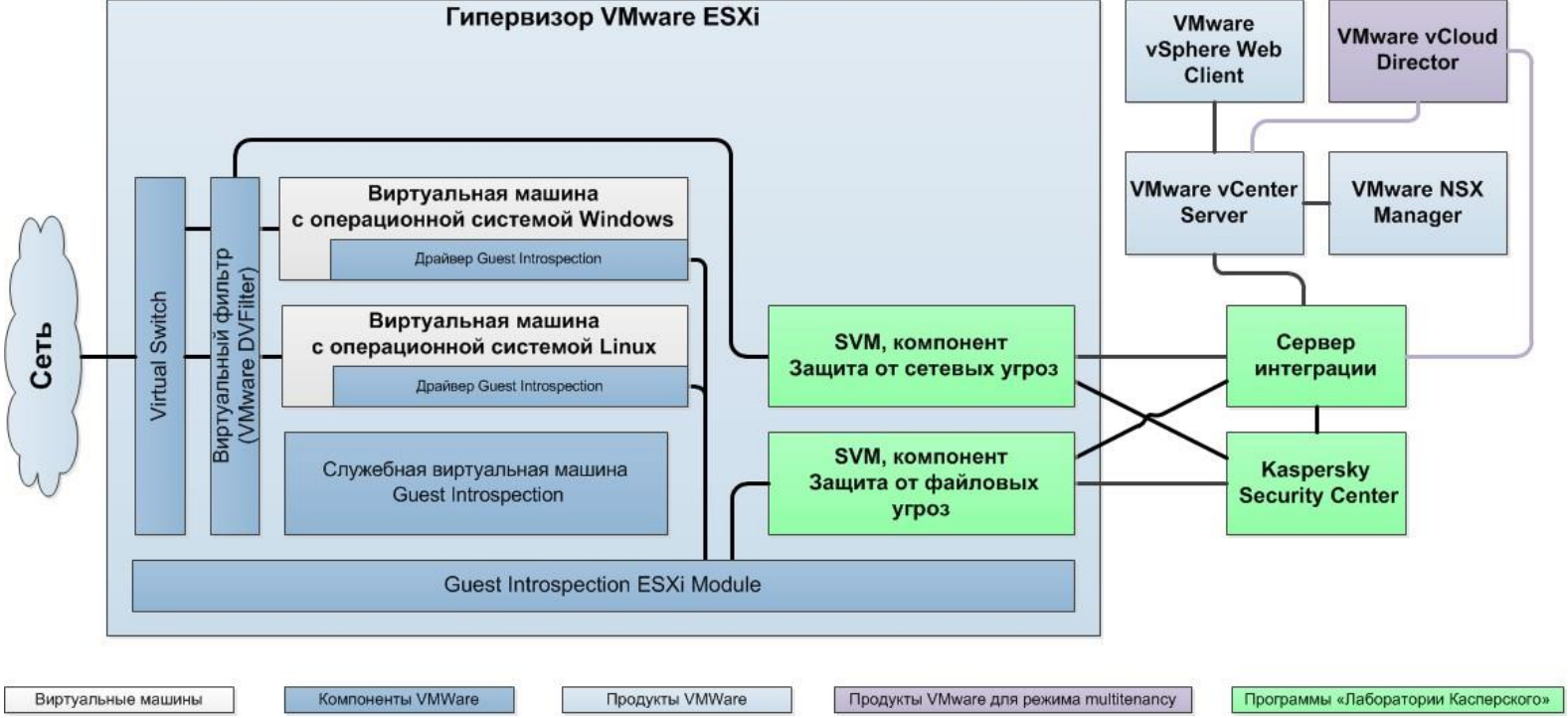
Архитектура программы

Kaspersky Security поставляется в виде двух образов SVM (виртуальной машины защиты):

- образа SVM с установленным компонентом Защита от файловых угроз; образа SVM с
- установленным компонентом Защита от сетевых угроз.

SVM (secure virtual machine, виртуальная машина защиты) – виртуальная машина, на которой установлен компонент программы Kaspersky Security. SVM разворачиваются на гипервизоре VMware ESXi. Для обеспечения защиты и проверки виртуальных машин не требуется устанавливать программу на каждую виртуальную машину.

Компоненты Kaspersky Security регистрируются в VMware NSX Manager как службы:



- компонент Защита от файловых угроз – как служба защиты файловой системы (Kaspersky File Antimalware Protection);
- компонент Защита от сетевых угроз – как служба сетевой защиты (Kaspersky Network Protection).

Службы Kaspersky Security разворачиваются на кластере VMware в ходе установки программы. В результате развертывания служб Kaspersky Security на каждом гипервизоре в составе кластера разворачиваются SVM с компонентами Kaspersky Security (см. рис. ниже).

Архитектура программы

SVM с компонентом Защита от файловых угроз обеспечивают:

- защиту от вирусов и других вредоносных программ всех виртуальных машин, для которых выполняются условия защиты виртуальных машин;
- антивирусную проверку файлов всех виртуальных машин, для которых выполняются условия проверки виртуальных машин.

SVM с компонентом Защита от сетевых угроз обеспечивают защиту от сетевых угроз всех виртуальных машин, для которых выполняются условия защиты виртуальных машин от сетевых угроз.

Взаимодействие между виртуальной инфраструктурой VMware и компонентами программы Kaspersky Security обеспечивает компонент Сервер интеграции.

Управление работой программы осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center. Взаимодействие программы Kaspersky Security с программой Kaspersky Security Center обеспечивает Агент администрирования, который является компонентом Kaspersky Security Center. Агент администрирования включен в состав образа SVM.

Интерфейс для управления программой Kaspersky Security через Kaspersky Security Center обеспечивает основной плагин управления Kaspersky Security. Если программа работает в режиме multitenancy, для управления программой также требуется плагин управления Kaspersky Security для клиентов.

Плагины управления Kaspersky Security входят в комплект поставки Kaspersky Security.

Плагины управления Kaspersky Security должны быть установлены на том компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

Состав образов SVM Kaspersky Security

В состав образа SVM с установленным компонентом Защита от файловых угроз входят:

- Операционная система CentOS 7.6.
- Компонент Kaspersky Security Защита от файловых угроз.
- Библиотека EPSEC – компонент, предоставленный компанией VMware. Библиотека EPSEC обеспечивает доступ к файлам тех виртуальных машин, которые защищает Kaspersky Security.
- Агент администрирования – компонент Kaspersky Security Center. Агент администрирования осуществляет взаимодействие с Сервером администрирования Kaspersky Security Center, позволяя Kaspersky Security Center управлять программой Kaspersky Security.

В состав образа SVM с установленным компонентом Защита от сетевых угроз входят:

- Операционная система CentOS 7.6.
- Компонент Kaspersky Security Защита от сетевых угроз.
- Guest Introspection SDK – компонент, предоставленный компанией VMware. Guest Introspection SDK обеспечивает возможность мониторинга сетевого трафика виртуальных машин на уровне сетевых пакетов и возможность создавать виртуальные фильтры.
- Агент администрирования – компонент Kaspersky Security Center. Агент администрирования осуществляет взаимодействие с Сервером администрирования Kaspersky Security Center, позволяя Kaspersky Security Center управлять программой Kaspersky Security.

Варианты использования программы

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

SVM с компонентами Kaspersky Security разворачиваются на гипервизорах VMware ESXi под управлением одного или нескольких автономных серверов VMware vCenter Server и обеспечивают защиту виртуальных машин, работающих на этих гипервизорах. Программа работает в обычном режиме.

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

Защита виртуальной инфраструктуры под управлением VMware vCloud Director

SVM с компонентами Kaspersky Security разворачиваются на гипервизорах VMware ESXi под управлением серверов VMware vCenter Server, подключенных к серверу VMware vCloud Director. SVM могут защищать все виртуальные машины, работающие в виртуальной инфраструктуре, в том числе виртуальные машины, которые входят в организации vCloud Director.

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

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

Для управления защитой клиентов используются виртуальные Серверы администрирования Kaspersky Security Center. Администратор провайдера создает для каждого клиента отдельный виртуальный Сервер администрирования и предоставляет администратору клиента доступ к нему. С помощью виртуального Сервера администрирования и плагина управления для клиентов администратор клиента может управлять защитой своей виртуальной инфраструктуры от файловых угроз. Управление сетевой защитой, а также обновление баз программы, активацию программы и работу с копиями файлов, помещенных в резервное хранилище, обеспечивает провайдер.

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

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

Интеграция компонентов Kaspersky Security с виртуальной инфраструктурой VMware

Для интеграции компонентов Kaspersky Security с виртуальной инфраструктурой VMware требуется следующее:

- Сервер управления виртуальной инфраструктурой (VMware vCenter Server, VMware vCloud Director). Компонент предназначен для администрирования и централизованного управления виртуальной инфраструктурой VMware. Компонент участвует в развертывании Kaspersky Security. Сервер интеграции получает от сервера управления виртуальной инфраструктурой информацию о виртуальной инфраструктуре VMware, необходимую для работы программы.

- VMware NSX Manager. Компонент обеспечивает регистрацию и развертывание служб Kaspersky Security.

- Виртуальный фильтр (VMware DVFilter). Компонент позволяет перехватывать входящие и исходящие сетевые пакеты в трафике защищенных виртуальных машин.

- Драйвер Guest Introspection (NSX File Introspection Driver). Компонент обеспечивает сбор информации на виртуальных машинах и передачу файлов на проверку программе Kaspersky Security. Чтобы программа Kaspersky Security имела возможность защищать виртуальные машины, на этих виртуальных машинах требуется установить NSX File Introspection Driver. См. подробнее в документации к продуктам VMware.

- Служба Guest Introspection и Guest Introspection ESXi Module. Компоненты обеспечивают взаимодействие между драйвером Guest Introspection, установленным на виртуальной машине, и SVM.

Компонент Защита от файловых угроз взаимодействует с виртуальной инфраструктурой VMware по следующей схеме:

. Пользователь или какая-либо программа открывает, сохраняет или запускает файлы на виртуальной машине, которая находится под защитой Kaspersky Security.

. Драйвер Guest Introspection перехватывает информацию об этих событиях и отправляет службе Guest Introspection.

. Служба Guest Introspection передает информацию о полученных событиях компоненту Защита от файловых угроз, установленному на SVM.

. Компонент Защита от файловых угроз проверяет файлы, которые пользователь или какая-либо программа открывает, сохраняет или запускает на защищенной виртуальной машине:

  - Если в файлах не обнаружены вирусы или другие вредоносные программы, Kaspersky Security разрешает доступ к этим файлам.

  - Если в файлах обнаружены вирусы или другие вредоносные программы, Kaspersky Security выполняет то действие, которое указано в параметрах профиля защиты, назначенного этой виртуальной машине. Например, Kaspersky Security лечит или блокирует файл.

Взаимодействие компонента Защита от сетевых угроз с виртуальной инфраструктурой VMware зависит от режима обработки трафика, который вы выбрали при регистрации службы сетевой защиты (Kaspersky Network Protection). Если вы выбрали стандартный режим обработки трафика, компонент Защита от сетевых угроз взаимодействует с виртуальной инфраструктурой VMware по следующей схеме:

. Виртуальный фильтр (VMware DVFilter) перехватывает входящие и исходящие сетевые пакеты в трафике защищенных виртуальных машин и перенаправляет их компоненту Защита от сетевых угроз, установленному на SVM.

. Компонент Защита от сетевых угроз проверяет сетевые пакеты на наличие активности, характерной для сетевых атак, и подозрительной сетевой активности, которая может быть признаком вторжения в защищаемую инфраструктуру, а также проверяет все веб-адреса в запросах по протоколу HTTP на принадлежность к категориям веб-адресов, которые требуется обнаруживать в соответствии с параметрами проверки вебадресов.

  Если в сетевом пакете не обнаружена сетевая атака или подозрительная сетевая активность и веб-адрес не принадлежит ни к одной из категорий веб-адресов, выбранных для обнаружения, Kaspersky Security разрешает произвести передачу сетевого пакета.

  Если сетевая угроза обнаружена, Kaspersky Security выполняет следующие действия:

  - Если обнаружена активность, характерная для сетевых атак, Kaspersky Security выполняет то действие, которое указано в параметрах политики. Например, Kaspersky Security блокирует или пропускает сетевые пакеты, поступающие с IP-адреса, с которого произведена сетевая атака.

- Если обнаружена подозрительная сетевая активность, Kaspersky Security выполняет то действие, которое указано в параметрах политики. Например, Kaspersky Security блокирует или пропускает сетевые пакеты, поступающие с IP-адреса, с которого произведена сетевая атака.

- Если веб-адрес принадлежит к одной или нескольким категориям веб-адресов, выбранным для обнаружения, Kaspersky Security выполняет то действие, которое указано в параметрах политики. Например, Kaspersky Security блокирует или разрешает доступ к веб-адресу.

Если при регистрации службы сетевой защиты (Kaspersky Network Protection) вы выбрали режим мониторинга, компонент Защита от сетевых угроз получает копию трафика виртуальных машин. При обнаружении признаков вторжений или попыток доступа к опасным или нежелательным веб-адресам Kaspersky Security не предпринимает действий по предотвращению угроз, а только передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

О Сервере интеграции

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

Сервер интеграции используется для выполнения следующих задач:

- Регистрация в VMware NSX Manager служб Kaspersky Security: службы защиты файловой системы (Kaspersky File Antimalware Protection) и службы сетевой защиты (Kaspersky Network Protection). Службы Kaspersky Security необходимы для установки компонентов программы в инфраструктуре VMware.

  Ввод параметров, необходимых для регистрации и развертывания служб Kaspersky Security, выполняется с помощью мастера, который запускается из Консоли Сервера интеграции.

- Настройка конфигурации новых SVM и изменение конфигурации ранее развернутых SVM. Сервер интеграции передает на SVM параметры, которые вы задали в Консоли Сервера интеграции.

- Получение от сервера VMware vCenter Server и передача компонентам программы информации о виртуальной инфраструктуре (о гипервизорах и виртуальных машинах, работающих на каждом гипервизоре). Плагин управления Kaspersky Security и SVM в ходе своей работы обращаются к Серверу интеграции для получения информации о виртуальной инфраструктуре.

- Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center. Если вы используете программу Kaspersky Security в режиме multitenancy, для защиты виртуальной инфраструктуры каждой организации-клиента требуется установить соответствие между организацией vCloud Director, которая содержит виртуальные машины клиента, и виртуальным Сервером администрирования. Настройка списка соответствий выполняется в Консоли Сервера интеграции.

Во время работы Сервер интеграции сохраняет следующую информацию:

- параметры подключения к Серверу интеграции, в том числе пароли учетных записей Сервера интеграции;

- параметры подключения Сервера интеграции к VMware vCenter Server и VMware NSX Manager; параметры

- конфигурации SVM, в том числе пароли учетных записей root и klconfig, используемые на SVM;

-

список защищаемых виртуальных машин с указанием времени последних событий, произошедших в ходе защиты, проверки объектов файловой системы, проверки сетевого трафика и веб-адресов.

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

О Консоли Сервера интеграции

Консоль Сервера интеграции содержит следующие разделы:

Раздел Параметры Сервера интеграции

В этом разделе вы можете посмотреть информацию о Сервере интеграции.

Раздел Учетные записи Сервера интеграции

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

Раздел Защита виртуальной инфраструктуры

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

В таблице отображаются все серверы управления виртуальной инфраструктурой (VMware vCenter Server и VMware vCloud Director), к которым настроено подключение для Сервера интеграции.

Над таблицей расположены следующие кнопки:

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

- Кнопка Обновить позволяет обновить статус взаимодействия Сервера интеграции с виртуальной инфраструктурой.

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

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера VMware vCenter Server.

- Блок параметров, который содержит сообщения об ошибках подключения (если они есть) и список действий, которые вы можете выполнить при настройке подключения к этому VMware vCenter Server и для дальнейшего развертывания защиты виртуальной инфраструктуры под управлением этого VMware vCenter Server. Вы можете развернуть или свернуть список возможных действий для каждого сервера VMware vCenter Server щелчком левой клавиши мыши по адресу или имени сервера.

- Информация о развертывании защиты на кластерах VMware под управлением этого сервера VMware vCenter Server в виде N/M, где:
    - N – количество гипервизоров VMware ESXi, на которых развернута служба защиты файловой системы (Kaspersky File Antimalware Protection), или прочерк, если служба не зарегистрирована в VMware NSX Manager;
    - M – количество гипервизоров VMware ESXi, на которых развернута служба сетевой защиты (Kaspersky Network Protection), или прочерк, если служба не зарегистрирована в VMware NSX Manager.

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

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

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

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

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

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

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

Также в таблице отображается предупреждение, если в одной или нескольких политиках безопасности NSX, в которых настроено использование служб Kaspersky Security, выключено перенаправление трафика службе сетевой защиты (Kaspersky Network Protection). Если вы хотите защищать виртуальные машины от сетевых угроз, вам нужно включить перенаправление трафика службе сетевой защиты в политиках безопасности NSX (параметр Redirect to service).

Список возможных действий для VMware vCenter Server:

- Зарегистрировать службы Kaspersky Security – запускает мастер, с помощью которого вы можете ввести параметры, необходимые для регистрации в VMware NSX Manager и развертывания служб Kaspersky Security на кластерах VMware, а

также для настройки конфигурации новых SVM. По окончании ввода параметров Сервер интеграции выполняет регистрацию служб Kaspersky Security в VMware NSX Manager.

- Изменить параметры Kaspersky Security – запускает мастер, с помощью которого вы можете изменить параметры подключений для взаимодействия Сервера интеграции с VMware NSX Manager, указать или изменить образы SVM для службы защиты файловой системы (Kaspersky File Antimalware Protection) и / или службы сетевой защиты (Kaspersky Network Protection), а также изменить параметры конфигурации SVM, которые применяются на новых SVM и на ранее развернутых SVM. По окончании ввода параметров Сервер интеграции применяет новые параметры и, если требуется, выполняет повторную регистрацию служб Kaspersky Security в VMware NSX Manager.

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

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

- Изменить параметры подключения к VMware vCenter Server – открывает окно Подключение к виртуальной инфраструктуре, в котором вы можете изменить параметры подключения Сервера интеграции к VMware vCenter Server.

- Удалить VMware vCenter Server из списка – открывает окно, в котором вы можете подтвердить удаление параметров подключения Сервера интеграции к этому VMware vCenter Server. Сервер VMware vCenter Server будет удален из списка серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

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

Список возможных действий для VMware vCloud Director:

- Установить соответствия для организаций vCloud Director – открывает окно Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования, в котором вы можете установить соответствие между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования Kaspersky Security Center.

- Изменить параметры подключения к VMware vCloud Director – открывает окно Подключение к виртуальной инфраструктуре, в котором вы можете изменить параметры подключения Сервера интеграции к VMware vCloud Director.

- Удалить VMware vCloud Director из списка – открывает окно, в котором вы можете подтвердить удаление параметров подключения Сервера интеграции к этому VMware vCloud Director. Сервер VMware vCloud Director будет удален из списка серверов управления виртуальной инфраструктурой, к которым подключается Сервер интеграции.

Раздел Управление защитой организаций-клиентов

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

В этом разделе вы можете выполнить следующие действия:

- Подключить Сервер интеграции к Серверу администрирования Kaspersky Security Center.

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

- Посмотреть или настроить список соответствий между организациями vCloud Director, которые содержат виртуальные машины клиентов, и виртуальными Серверами администрирования Kaspersky Security Center.

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

Об обработке данных

Во время работы компоненты программы Kaspersky Security могут сохранять и передавать другим компонентам программы, а также программе Kaspersky Security Center следующую информацию, которая может содержать персональные данные:

- Для формирования отчетов и событий SVM передают Серверу администрирования Kaspersky Security Center информацию о работе программы. В том числе могут передаваться имена обработанных файлов и пути к ним в файловой системе, имена и адреса виртуальных машин, обработанные веб-адреса.

- Для обеспечения возможности работы через Kaspersky Security Center с объектами резервного хранилища SVM передают Серверу администрирования Kaspersky Security Center информацию об объектах, помещенных в резервное хранилище. В том числе могут передаваться имя объекта и путь к нему в файловой системе. По запросу администратора в Kaspersky Security Center могут быть переданы и объекты, помещенные в резервное хранилище.

- В ходе выполнения задач SVM передают Серверу администрирования Kaspersky Security Center информацию о параметрах и результатах выполнения задач.

- Для отображения в Консоли администрирования Kaspersky Security Center SVM передают Серверу администрирования Kaspersky Security Center список защищаемых виртуальных машин. В том числе могут передаваться имя защищаемой виртуальной машины и путь к ней в виртуальной инфраструктуре.

- SVM получают от Сервера администрирования Kaspersky Security Center параметры работы, заданные с помощью политик. В том числе могут передаваться пути к файлам, веб-адреса.

- В ходе настройки конфигурации SVM Сервер интеграции передает SVM пароли учетных записей root и klconfig, заданные пользователем, параметры подключения к сетевому хранилищу данных для SVM, IP-адрес Сервера интеграции, а также параметры подключения к Серверу интеграции и Серверу администрирования Kaspersky Security Center.

- Для обеспечения работы программы Сервер интеграции получает от сервера VMware vCenter Server и передает SVM информацию о виртуальной инфраструктуре.

Указанная информация передается по зашифрованным каналам передачи данных.

Концепция управления программой через Kaspersky Security Center

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

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

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

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

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

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

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

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

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

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

Выбрав папку Кластеры и массивы серверов, вложенную в папку группы администрирования с названием кластера KSC, вы можете открыть окно свойств кластера. В окне свойств кластера KSC вы можете посмотреть:

- список SVM, входящих в состав этого кластера KSC (раздел Узлы); список виртуальных машин в
- составе защищаемой инфраструктуры этого кластера KSC; список задач, созданных для SVM
- этого кластера KSC.

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

- Политика – это набор параметров работы программы, заданный для группы администрирования. В случае программы Kaspersky Security политика применяется на SVM и определяет параметры, с которыми SVM защищают виртуальные машины, которые находятся в области действия политики.

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

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

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

О политиках Kaspersky Security

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

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

Типы политик Kaspersky Security

Для программы Kaspersky Security предусмотрены политики следующих типов:

- Основная политика. Позволяет настраивать параметры защиты виртуальных машин от файловых угроз с помощью профилей защиты, параметры защиты от сетевых угроз, а также следующие параметры работы программы:
  - параметры уведомлений о событиях в работе программы;
  - параметры резервного хранилища; параметры использования
  - Kaspersky Security Network; параметры SNMP-мониторинга.
  - Если программа работает в режиме multitenancy, основная политика определяет параметры защиты от сетевых угроз для всех виртуальных машин и параметры защиты от файловых угроз для виртуальных машин, которые не входят в состав организаций vCloud Director.

  Основные политики рекомендуется создавать на главном Сервере администрирования Kaspersky Security Center. Основные политики создаются с помощью основного плагина управления Kaspersky Security.

- Политика для клиентов (используется, только если программа работает в режиме multitenancy). Позволяет настраивать параметры защиты для виртуальных машин, которые входят в состав организаций vCloud Director. С помощью этой политики вы можете задавать следующие параметры:

  - параметры уведомлений о событиях, произошедших во время защиты и проверки виртуальных машин клиента (только в политике, которая создана на главном Сервере администрирования Kaspersky Security Center);
  - индивидуальные параметры файловой защиты для виртуальных машин клиента; параметры использования KSN для организации-клиента.

  Вы можете создавать политики для клиентов на главном или на виртуальных Серверах администрирования Kaspersky Security Center с помощью плагина управления Kaspersky Security для клиентов.

Защищаемая инфраструктура политики

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

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

Область применения политики

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

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

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

Наследование параметров политик

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

параметров "замок" закрыт ( ), значения этих параметров записываются в политиках вложенного уровня иерархии и переопределить эти значения невозможно.

О профилях защиты Kaspersky Security

В политиках Kaspersky Security предусмотрены следующие профили защиты:

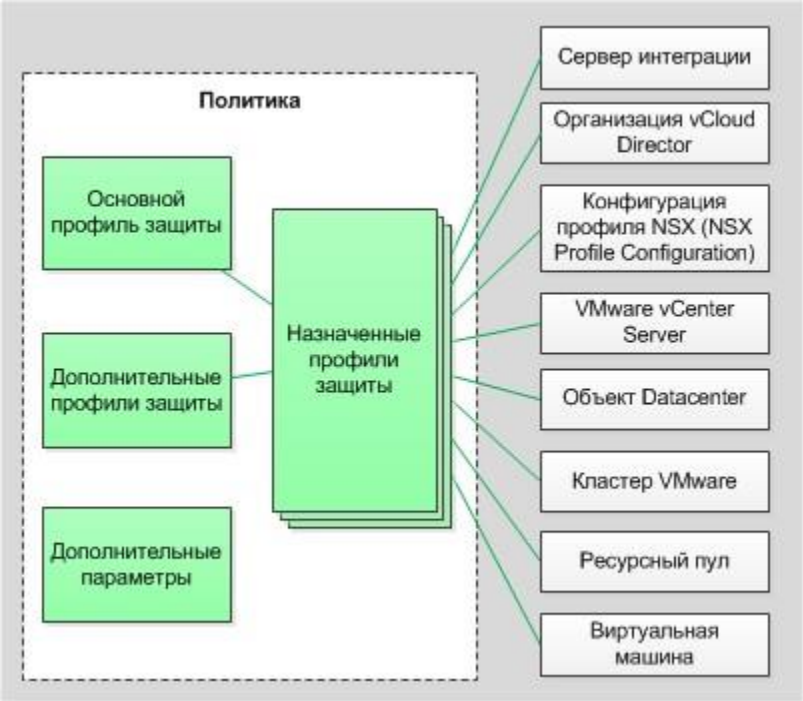
- Основной профиль защиты автоматически формируется во время создания политики. Основной профиль защиты недоступен для удаления, однако вы можете изменять значения параметров основного профиля защиты.

- Дополнительные профили защиты вы можете создать после создания политики. Благодаря дополнительным профилям защиты вы можете гибко настраивать разные параметры защиты для разных виртуальных машин в составе защищаемой инфраструктуры. Политика может содержать несколько дополнительных профилей защиты.

В профилях защиты вы можете настраивать следующие параметры защиты от файловых угроз:

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

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



Профили защиты

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

В основной политике, которая определяет параметры защиты виртуальной инфраструктуры под управлением одного сервера VMware vCenter Server, вы можете непосредственно назначать профили защиты объектам виртуальной инфраструктуры или использовать конфигурации профилей NSX (NSX Profile Configurations) для назначения параметров файловой защиты.

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

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

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

Об управлении политиками

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

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

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

Чтобы открыть окно свойств политики, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана политика.

. В рабочей области выберите закладку Политики.

. В списке политик выберите политику и откройте окно Свойства: <Название политики> двойным щелчком мыши по политике или выбрав в контекстном меню пункт Свойства.

Вы также можете выполнять следующие действия с политиками:

- копировать политики из одной папки или группы администрирования в другую;
- экспортировать политики в файл и импортировать политики из файла; конвертировать
- политики предыдущей версии программы; удалять политики.
- Подробнее об управлении политиками см. в документации Kaspersky Security Center.

Особенности использования политик Kaspersky Security

Основная политика в папке Управляемые устройства главного Сервера администрирования

Такая политика автоматически создается с помощью мастера первоначальной настройки управляемой программы после установки основного плагина управления Kaspersky Security. Вы также можете создать такую политику вручную с помощью мастера создания политики.

Политика применяется на всех SVM всех кластеров KSC.

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

В области действия этой политики находятся следующие виртуальные машины:

- файловая защита распространяется на все виртуальные машины в составе защищаемой инфраструктуры политики, кроме виртуальных машин, которые входят в состав организаций vCloud Director;
- сетевая защита распространяется на все виртуальные машины в составе защищаемой инфраструктуры политики (в том числе виртуальные машины, которые входят в состав организаций vCloud Director).

Файловая и сетевая защита по умолчанию выключены.

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

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

Чтобы включить сетевую защиту, вам нужно настроить параметры предотвращения вторжений и проверки вебадресов в свойствах политики.

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

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

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

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

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

Сетевая защита по умолчанию выключена. Чтобы включить сетевую защиту, вам нужно настроить параметры предотвращения вторжений и проверки веб-адресов в свойствах политики.

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

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

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

В области действия этой политики находятся следующие виртуальные машины:

- файловая защита распространяется на все виртуальные машины в составе защищаемой инфраструктуры кластера "VMware vCloud Director Agentless", которые не входят в состав организаций vCloud Director;
- сетевая защита распространяется на все виртуальные машины в составе защищаемой инфраструктуры кластера "VMware vCloud Director Agentless", в том числе виртуальные машины, которые входят в состав организаций vCloud Director.

Файловая и сетевая защита по умолчанию выключены.

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

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

Чтобы включить сетевую защиту, вам нужно настроить параметры предотвращения вторжений и проверки вебадресов в свойствах политики.

Политика для клиентов в папке Управляемые устройства главного Сервера администрирования

Такая политика автоматически создается с помощью мастера первоначальной настройки управляемой программы после установки плагина управления Kaspersky Security для клиентов на главном Сервере администрирования. Вы также можете создать такую политику вручную с помощью мастера создания политики.

Если в папке Управляемые устройства главного Сервера администрирования отсутствует политика для клиентов, в Kaspersky Security Center не регистрируются события, которые произошли во время проверки и защиты виртуальных машин клиентов, а также не отображаются виртуальные машины клиентов в составе защищаемой инфраструктуры кластера KSC и в списке виртуальных машин, находящихся под защитой SVM.

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

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

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

Если вы хотите централизовано включить использование Kaspersky Security Network для защиты всех виртуальных машин клиентов, вам нужно предварительно получить согласие клиентов на отправку в "Лабораторию Касперского" информации об использовании KSN, а также другой информации в зависимости от выбранного вами режима использования KSN (стандартный KSN или расширенный KSN).

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

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

Политика для клиентов в папке Управляемые устройства виртуального Сервера администрирования Вы можете

создать такую политику вручную с помощью мастера создания политики.

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

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

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

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

О задачах Kaspersky Security

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

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

- Глобальная задача – задача для одной или нескольких SVM, независимо от их нахождения в группе администрирования.

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

Для Kaspersky Security предусмотрены следующие задачи:

- задачи полной и выборочной проверки, которые позволяют выполнять проверку всех или только указанных виртуальных машин, находящихся в области действия задачи;

- служебные задачи, которые позволяют активировать программу, обновлять базы программы, откатывать обновления, устанавливать патчи программы.

Задача полной проверки

Задача полной проверки позволяет выполнять антивирусную проверку файлов всех виртуальных машин, находящихся в области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

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

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

Задача полной проверки, созданная с помощью основного плагина управления

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

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

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

Задача полной проверки, созданная с помощью плагина управления для клиентов

Создание задачи полной проверки для виртуальных машин клиентов поддерживается только на виртуальном Сервере администрирования Kaspersky Security Center. Вы можете создать задачу полной проверки с помощью плагина управления Kaspersky Security для клиентов в папке Управляемые устройства виртуального Сервера администрирования. В области действия этой задачи находятся все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования.

Задача выборочной проверки

Задача выборочной проверки позволяет выполнять антивирусную проверку файлов указанных виртуальных машин из области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

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

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

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

Задача выборочной проверки, созданная с помощью основного плагина управления

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

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

- если вы хотите проверять виртуальные машины под управлением автономного сервера VMware vCenter Server, вам нужно создать задачу в группе, которая содержит кластер "VMware vCenter Agentless", соответствующий этому VMware vCenter Server и указать в качестве области действия задачи этот сервер VMware vCenter Server.

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

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

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

Задача выборочной проверки, созданная с помощью плагина управления для клиентов

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

Служебные задачи

Для управления программой вы можете использовать следующие служебные задачи:

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

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

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

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

Об управлении задачами

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

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

Чтобы открыть окно свойств задачи, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана задача.

. В рабочей области выберите закладку Задачи.

. В списке задач выберите задачу и откройте окно Свойства: <Название задачи> двойным щелчком мыши по задаче или выбрав в контекстном меню пункт Свойства.

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

Чтобы запустить или остановить задачу, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой создана задача.
. В рабочей области выберите закладку Задачи.

. В списке задач выберите задачу, которую вы хотите запустить или остановить.

. Нажмите на кнопку Запустить или на кнопку Остановить. Кнопки расположены справа от списка задач.

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

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

Вы также можете выполнять следующие действия с задачами:

- копировать задачи из одной папки или группы администрирования в другую;
- экспортировать задачи в файл и импортировать задачи из файла; конвертировать
- задачи предыдущей версии программы; удалять задачи.
- Подробнее об управлении задачами см. в документации Kaspersky Security Center.

О правах доступа к параметрам политик и задач

Права на доступ к параметрам политик и задач (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center. В Консоли администрирования Kaspersky Security Center вы можете назначать учетным записям пользователей права на выполнение определенных действий в функциональных областях программы Kaspersky Security.

Выделены следующие функциональные области Kaspersky Security:

- Антивирусная защита. В эту функциональную область входят следующие параметры и функции:
  - Включение и выключение функции антивирусной защиты.
  - Все параметры уровня безопасности в политиках:
    - Проверка архивов, самораспаковывающихся архивов и вложенных OLE-объектов.
    - Проверка составных файлов большого размера.
    - Ограничение на время проверки файла.
    - Список обнаруживаемых объектов.
  - Действие, которое выполняет Kaspersky Security при обнаружении зараженных файлов во время защиты виртуальных машин.

- Проверка файлов на сетевых дисках во время защиты виртуальных машин.
- Включение и выключение функции проверки веб-адресов.
- Список категорий веб-адресов, которые обнаруживает Kaspersky Security.
- Действие, которое выполняет Kaspersky Security, если устанавливает принадлежность веб-адреса к одной или нескольким категориям веб-адресов, выбранных для обнаружения.
- Параметры резервного хранилища.
- Параметры использования KSN.
- Список дополнительных профилей защиты в политике.
- Назначение и изменение защищаемой инфраструктуры для политики.
- Назначение профилей защиты объектам виртуальной инфраструктуры VMware.
- Задачи полной проверки и задачи выборочной проверки.

- Базовая функциональность. В эту функциональную область входят следующие параметры и функции:
  - Параметры SNMP-мониторинга.
  - Язык сообщения о блокировке веб-адреса, которое отображается в браузере на защищенной виртуальной машине.
  - Задача обновления баз программы и задача отката последнего обновления баз программы.
  - Задача активации программы.
  - Задача автоматической установки патчей.
- Предотвращение вторжений. В эту функциональную область входят следующие параметры и функции:
  - Включение и выключение функции обнаружения сетевых атак.
  - Действие, которое выполняет Kaspersky Security при обнаружении сетевой атаки.
  - Включение и выключение контроля сетевой активности виртуальных машин.
  - Действие, которое выполняет Kaspersky Security при обнаружении подозрительной сетевой активности.
  - Список категорий программ, признаки сетевой активности которых обнаруживает Kaspersky Security.
  - Продолжительность блокировки IP-адреса, который является источником сетевой атаки или подозрительной сетевой активности.
- Доверенная зона. В эту функциональную область входят следующие параметры и функции:

- Список расширений файлов, исключаемых из защиты.
- Список расширений файлов, включаемых в область действия защиты.
- Список папок и файлов, исключаемых из защиты.
- Список правил выявления подозрительной сетевой активности, которые Kaspersky Security не применяет во время анализа трафика защищенных виртуальных машин.
- Список правил исключения из защиты от сетевых угроз.
- Список веб-адресов, доступ к которым Kaspersky Security не блокирует независимо от настроенных параметров проверки веб-адресов.

Следующие действия доступны пользователю независимо от прав учетной записи в функциональных областях программы Kaspersky Security:

- Просмотр параметров политик и задач.
- Создание политики.

Права в функциональных областях программы Kaspersky Security требуются для выполнения следующих действий с политиками и задачами:

- Для изменения параметров ранее сохраненной политики учетная запись пользователя должна обладать правами на изменение в функциональных областях, к которым относятся эти параметры.
- Для изменения состояния политики (активная / неактивная) и удаления политики учетная запись пользователя должна обладать правами на изменение в функциональных областях, к которым относятся все параметры политики. Если у учетной записи пользователя нет прав на редактирование какого-либо параметра политики, то удаление или изменение состояния политики невозможно.
- Для создания, удаления и настройки параметров задач учетная запись пользователя должна обладать правами на изменение в функциональной области, к которой относится задача.
- Для запуска задачи учетная запись пользователя должна обладать правами на выполнение в функциональной области, к которой относится задача.

Настройка доступа к функциональным областям Kaspersky Security выполняется в окне свойств Сервера администрирования Kaspersky Security Center в разделе Безопасность.

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

Подробнее о правах доступа к объектам Kaspersky Security Center см. в документации Kaspersky Security Center.

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 программы Kaspersky Security.
- Подготовить виртуальную инфраструктуру VMware к установке программы.
- Загрузить с веб-сайта "Лаборатории Касперского" все файлы образов SVM.
- Убедиться в том, что образы SVM получены из доверенного источника. Подробнее о способах проверки подлинности образа SVM см. на странице программы в Базе знаний.
- Разместить все файлы образов SVM в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS. Например, вы можете опубликовать образы SVM на Веб-сервере Kaspersky Security Center.
- В настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика, открыть порты, которые требуются для работы программы.
- Настроить параметры учетных записей, которые требуются для установки и работы программы.
- Если вы планируете использовать сетевое хранилище данных для SVM, создать сетевую папку для размещения сетевого хранилища данных и учетную запись для подключения SVM. Сетевое хранилище данных используется для хранения резервных копий файлов, помещенных в резервные хранилища на SVM. Место, которое требуется для сетевого хранилища данных, можно оценить по формуле: (N+1) ГБ, где N – количество SVM, которые подключаются к сетевому хранилищу данных.

Подготовка виртуальной инфраструктуры VMware

Перед установкой программы в инфраструктуре VMware требуется выполнить следующие действия:

- Объединить гипервизоры VMware ESXi в один или несколько кластеров VMware.
- Настроить в свойствах каждого гипервизора параметры Agent VM Settings: выбрать сеть и хранилище для служебных виртуальных машин и SVM. Подробнее о настройке параметров Agent VM Settings см. в документации к продуктам VMware.
- На каждом кластере VMware, на котором будут развернуты SVM с компонентом Защита от файловых угроз, развернуть службу Guest Introspection.
- На каждом кластере VMware, на котором будут развернуты SVM с компонентом Защита от сетевых угроз, подготовить гипервизоры для развертывания сетевой защиты. Для этого нужно установить компоненты VMware NSX на гипервизорах. Установка выполняется в консоли VMware vSphere Web Client в разделе Networking & Security → Installation and Upgrade на закладке Host Preparation. Для установки компонентов VMware NSX на гипервизоры нужно для кластера VMware выполнить действие Actions → Install. См. подробнее в Базе знаний.
- Установить драйвер Guest Introspection (NSX File Introspection Driver) на каждой виртуальной машине, которую вы хотите защищать с помощью Kaspersky Security.

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

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

- Если вы хотите установить компонент Защита от сетевых угроз, убедиться, что для VMware NSX for vSphere используется лицензия NSX for vSphere Advanced или NSX for vSphere Enterprise.

Развертывание службы Guest Introspection

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

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

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

Чтобы развернуть службу Guest Introspection, выполните следующие действия:

. В консоли VMware vSphere Web Client запустите мастер развертывания сетевых служб и служб обеспечения защиты виртуальных машин (раздел Networking & Security → Installation and Upgrade закладка Service Deployments).

. С помощью мастера укажите следующие параметры развертывания службы Guest Introspection: a.

Выберите в таблице службу Guest Introspection.

b. Выберите один или несколько кластеров VMware, на которых вы хотите установить компонент Защита от файловых угроз.

c. Если требуется, измените заданные по умолчанию параметры для всех служебных виртуальных машин Guest Introspection, которые будут развернуты на гипервизорах в составе выбранного кластера VMware:

- Сеть, которую будут использовать служебные виртуальные машины.
- Хранилище для развертывания служебных виртуальных машин.
- Способ назначения IP-адресов. По умолчанию служебные виртуальные машины получают сетевые параметры по протоколу DHCP. Вы можете настроить статический пул IP-адресов, из которого будут назначаться IP-адреса служебных виртуальных машин.

. 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.

Просмотр информации о лицензии NSX for vSphere

Для функционирования компонента Защита от сетевых угроз требуется наличие действующей лицензии NSX for vSphere Advanced или NSX for vSphere Enterprise.

При использовании стандартной лицензии NSX for vSphere недоступна функция Network Service Insertion (Third Party Integration), которая необходима для включения защиты от сетевых угроз на гипервизорах VMware ESXi.

Информацию об используемых лицензиях вы можете посмотреть в консоли VMware vSphere Web Client в разделе Administration → Licenses на закладке Products (см. подробнее в Базе знаний).

Информацию о работе с лицензиями NSX for vSphere см. в документации к продуктам VMware.

Публикация образов SVM на Веб-сервере Kaspersky Security Center

Вы можете опубликовать образы SVM на Веб-сервере Kaspersky Security Center или разместить на другом сетевом ресурсе, доступном по протоколу HTTP или HTTPS.

Чтобы опубликовать образы SVM на Веб-сервере Kaspersky Security Center, выполните следующие действия:

. Убедитесь, что Веб-сервер запущен. Для этого запустите оснастку services.msc и проверьте, что служба Kaspersky Lab Web Server находится в состоянии Работает (Running).

. В папке общего доступа Сервера администрирования создайте вложенную папку public.

Чтобы узнать путь к папке общего доступа, выполните следующие действия:

a. Посмотрите имя папки общего доступа и имя компьютера, на котором она расположена, в окне свойств Сервера администрирования в разделе Дополнительно → Папка общего доступа Сервера администрирования.

b. На указанном компьютере в командной строке выполните команду `net share <имя папки общего доступа>` .

В результате выполнения команды в строке `Path` выводится путь к папке общего доступа в файловой системе.

. Скопируйте в папку public все файлы образов SVM Kaspersky Security.

. Убедитесь, что образы SVM опубликованы. Для этого откройте браузер и введите в адресной строке `http://<IP-адрес Сервера администрирования Kaspersky Security Center>:8060/public`

В качестве адреса Сервера администрирования должен быть указан IP-адрес, не следует указывать localhost.

13000, 14000	От SVM к Серверу администрирования Kaspersky Security Center.	Для управления программой через Kaspersky Security Center.

Порт 8060 используется по умолчанию. Если вы изменили параметры по умолчанию, укажите в адресной строке порт, который задан в разделе Веб-сервер окна свойств Сервера администрирования Kaspersky Security Center.

Если публикация образов SVM завершилась успешно, откроется страница со списком файлов образов Kaspersky Security.

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.

Порты, используемые программой

Порт и	Направление	Назначение и описание протокол

Учетные записи для установки и работы программы

Учетная запись для установки плагина управления Kaspersky Security и Сервера интеграции

Для установки плагина управления Kaspersky Security и Сервера интеграции требуется учетная запись, которая обладает правами на установку программного обеспечения (например, учетная запись из группы локальных администраторов).

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

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

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

Учетные записи для развертывания, удаления SVM и работы программы

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

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

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

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

Учетная запись для подключения Сервера интеграции к Kaspersky Security Center

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

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

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

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

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

Учетная запись для подключения SVM к сетевому хранилищу данных

Эта учетная запись требуется, если вы используете сетевое хранилище данных для SVM. Сетевое хранилище данных используется для хранения резервных копий файлов, помещенных в резервные хранилища на SVM.

Для подключения SVM к сетевому хранилищу данных требуется учетная запись с правами на чтение и запись в сетевой папке, в которой расположено хранилище.

Рекомендуется ограничить доступ к этой сетевой папке для всех остальных учетных записей.

Установка программы

Установка программы Kaspersky Security состоит из следующих этапов:

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

Независимо от выбранного варианта использования программы вам нужно установить основной плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции.

Если вы хотите использовать программу в режиме multitenancy, вам нужно также установить плагин управления Kaspersky Security для клиентов.

При первом запуске Консоли администрирования Kaspersky Security Center после установки плагинов управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. Мастер позволяет создать политики по умолчанию и задачи.

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

. Настройка параметров подключения Сервера интеграции к одному или нескольким серверам управления виртуальной инфраструктурой.

. Регистрация в VMware NSX Manager служб Kaspersky Security.

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

Если вы хотите установить компонент Защита от сетевых угроз, вам нужно зарегистрировать службу сетевой защиты (Kaspersky Network Protection).

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

В консоли VMware vSphere Web Client вы можете убедиться в том, что регистрация служб Kaspersky Security завершилась успешно.

. Развертывание SVM с компонентом Защита от файловых угроз и SVM с компонентом Защита от сетевых угроз на гипервизорах VMware ESXi. Развертывание SVM выполняется в консоли VMware vSphere Web Client.

После развертывания SVM Сервер интеграции передает на каждую новую SVM параметры конфигурации, которые вы указали при регистрации служб Kaspersky Security.

Kaspersky Security Center помещает развернутые SVM в кластеры KSC.

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

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

a. Включить виртуальные машины в одну или несколько групп безопасности NSX (NSX Security Group).

b. Настроить одну или несколько политик безопасности NSX (NSX Security Policy) и применить политики безопасности на группы безопасности NSX.

. Подготовка программы к работе.

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

Если вы хотите использовать программу в режиме multitenancy, после установки программы вам нужно настроить защиту организаций-клиентов.

Установка основного плагина управления Kaspersky Security и Сервера интеграции

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

Вы можете установить основной плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции одним из следующих способов: в интерактивном режиме с помощью мастера; в тихом режиме из командной строки.

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

Основной плагин управления Kaspersky Security и Консоль Сервера интеграции должны быть установлены на том компьютере, где установлена Консоль администрирования Kaspersky Security Center. Сервер интеграции должен быть установлен на том компьютере, где установлен Сервер администрирования Kaspersky Security Center.

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

В зависимости от наличия установленных на компьютере компонентов Kaspersky Security Center после запуска установки выполняются следующие действия:

- Если на компьютере установлена только Консоль администрирования Kaspersky Security Center, устанавливаются плагин управления Kaspersky Security и Консоль Сервера интеграции.
- Если на компьютере установлены Сервер администрирования Kaspersky Security Center и Консоль администрирования Kaspersky Security Center, устанавливаются плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции.

Для взаимодействия Сервера интеграции с Консолью Сервера интеграции, с SVM, с VMware vCenter Server и VMware NSX Manager используется защищенное SSL-соединение. Для устранения известных уязвимостей операционной системы для протокола SSL при установке Сервера интеграции в реестр операционной системы вносятся изменения, описанные в базе технической поддержки Microsoft. 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 SSLсертификат Сервера интеграции, который используется для установки защищенного соединения с Сервером интеграции. Если требуется, вы можете заменить SSL-сертификат Сервера интеграции (процедура замены сертификата описана в Базе знаний).

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.

Установка в интерактивном режиме

Чтобы установить основной плагин управления Kaspersky Security и компоненты Сервера интеграции в интерактивном режиме с помощью мастера, выполните следующие действия:

. На компьютере, где установлены Консоль администрирования и Сервер администрирования Kaspersky Security Center, запустите файл ksv-components_6.0.0.XXX_mlg.exe, где 6.0.0.XXX – номер версии программы. Этот файл входит в комплект поставки.

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

Запустится мастер установки компонентов Kaspersky Security.

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

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

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

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

Перейдите к следующему шагу мастера.

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

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

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

Перейдите к следующему шагу мастера.

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

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

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

. Дождитесь завершения работы мастера.

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

. Нажмите на кнопку Завершить, чтобы закрыть окно мастера.

Информация о работе мастера записывается в файлы трассировки мастера установки компонентов Kaspersky Security. Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Установка из командной строки

Перед установкой плагина управления рекомендуется ознакомиться с текстом Лицензионного соглашения и Политики конфиденциальности. Для этого в командной строке введите следующую команду: `ksv-components_6.0.0.XXX_mlg.exe --lang=<идентификатор языка> --show-EulaAndPrivacyPolicy`

где `6.0.0.XXX` – номер версии программы.

Текст Лицензионного соглашения и Политики конфиденциальности выводится в файл EulaAndPrivacyPolicy_<идентификатор языка>.txt в папке %temp%.

Чтобы установить основной плагин управления Kaspersky Security и компоненты Сервера интеграции из командной строки,

в командной строке введите одну из следующих команд:

- если компьютер, на котором выполняется установка, входит в домен Active Directory:

  ```
  ksv-components_6.0.0.XXX_mlg.exe -q --lang=<идентификатор языка> --accept-EulaAndPrivacyPolicy=yes
  ```

- если компьютер, на котором выполняется установка, не входит в домен Active Directory:

  ```
  ksv-components_6.0.0.XXX_mlg.exe -q --lang=<идентификатор языка> --accept-EulaAndPrivacyPolicy=yes --viisPass=<пароль>
  ```

где:

- `6.0.0.XXX` – номер версии программы.
- `<идентификатор языка>` – идентификатор языка устанавливаемых компонентов.

  Идентификатор языка требуется указывать в следующем формате: ru, en, de, fr, zh-Hans, ja. Регистр символов учитывается.

- `<пароль>` – пароль для учетной записи администратора Сервера интеграции. Учетная запись администратора Сервера интеграции admin используется для управления Сервером интеграции, если компьютер, на котором установлен Сервер интеграции, не входит в домен Active Directory.

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

- `accept-EulaAndPrivacyPolicy=yes` означает, что вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, которая описывает обработку и передачу данных. Установив значение `yes`, вы подтверждаете следующее:
  - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения;
  - вы полностью прочитали и понимаете Политику конфиденциальности, вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

  Согласие с условиями Лицензионного соглашения и Политикой конфиденциальности является необходимым условием для установки плагина управления Kaspersky Security и компонентов Сервера интеграции.

По умолчанию для подключения к Серверу интеграции используется порт 7271. Если вы хотите использовать другой порт для подключения к Серверу интеграции, укажите в команде параметр `--viisPort=<номер порта из диапазона 1025-65536>`.

Установка основного плагина управления Kaspersky Security и компонентов Сервера интеграции занимает некоторое время. Информация о результате установки записывается в файлы трассировки мастера установки компонентов Kaspersky Security. Если установка завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Установка плагина управления Kaspersky Security для клиентов

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

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

Вы можете установить плагин управления Kaspersky Security для клиентов одним из следующих способов:

- в интерактивном режиме с помощью мастера; в
- тихом режиме из командной строки.

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

Плагин управления Kaspersky Security для клиентов должен быть установлен на том компьютере, где установлена Консоль администрирования Kaspersky Security Center.

Установка в интерактивном режиме

Чтобы установить плагин управления Kaspersky Security для клиентов в интерактивном режиме с помощью мастера, выполните следующие действия:

. На компьютере, где установлена Консоль администрирования Kaspersky Security Center, запустите файл ksv-tcomponents_6.0.0.XXX_mlg.exe, где 6.0.0.XXX – номер версии программы. Этот файл входит в комплект поставки.

Запустится мастер установки плагина управления Kaspersky Security для клиентов.

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

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

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

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

Перейдите к следующему шагу мастера.

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

. Дождитесь завершения работы мастера.

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

. Нажмите на кнопку Завершить, чтобы закрыть окно мастера.

Информация о работе мастера записывается в файлы трассировки мастера установки плагина управления Kaspersky Security для клиентов. Если работа мастера завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Установка из командной строки

Перед установкой плагина управления рекомендуется ознакомиться с текстом Лицензионного соглашения и Политики конфиденциальности. Для этого в командной строке введите следующую команду: `ksv-t-components_6.0.0.XXX_mlg.exe --lang=<идентификатор языка> --show-EulaAndPrivacyPolicy`

где `6.0.0.XXX` – номер версии программы.

Текст Лицензионного соглашения и Политики конфиденциальности выводится в файл EulaAndPrivacyPolicy_<идентификатор языка>.txt в папке %temp%.

Чтобы установить плагин управления Kaspersky Security для клиентов, в командной строке введите команду

```
ksv-t-components_6.0.0.XXX_mlg.exe -q --lang=<идентификатор языка> --accept-EulaAndPrivacyPolicy=yes
```

где:

- `6.0.0.XXX` – номер версии программы.
- `<идентификатор языка>` – идентификатор языка устанавливаемых компонентов.

  Идентификатор языка требуется указывать в следующем формате: ru, en, de, fr, zh-Hans, ja. Регистр символов учитывается.

- `accept-EulaAndPrivacyPolicy=yes` означает, что вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, которая описывает обработку и передачу данных. Установив значение `yes`, вы подтверждаете следующее:
  - вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения;
  -

вы полностью прочитали и понимаете Политику конфиденциальности, вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности.

Согласие с условиями Лицензионного соглашения и Политикой конфиденциальности является необходимым условием для установки плагина управления Kaspersky Security.

Информация о результате установки записывается в файлы трассировки мастера установки плагина управления Kaspersky Security для клиентов. Если установка завершилась с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Результат установки плагинов управления Kaspersky Security и Сервера интеграции

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

. В Консоли администрирования Kaspersky Security Center создается ссылка для запуска Консоли Сервера интеграции: Управление Kaspersky Kaspersky Security для виртуальных и облачных сред. Ссылка отображается в рабочей области узла Сервер администрирования на закладке Мониторинг в блоке Развертывание.

. При первом запуске Консоли администрирования Kaspersky Security Center после установки плагина управления запускается мастер первоначальной настройки управляемой программы, который создает в папке Управляемые устройства главного Сервера администрирования основную политику и задачи по умолчанию. Мастер также может быть запущен вручную.

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

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

. При первом запуске Консоли администрирования Kaspersky Security Center после установки плагина управления запускается мастер первоначальной настройки управляемой программы, который создает в папке Управляемые устройства главного Сервера администрирования политику для клиентов по умолчанию. Мастер также может быть запущен вручную.

. Плагин управления Kaspersky Security для клиентов отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

Просмотр списка установленных плагинов управления

Чтобы посмотреть список установленных плагинов управления, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. Откройте окно свойств Сервера администрирования одним из следующих способов:

- в контекстном меню узла выберите пункт Свойства;
- в рабочей области в блоке Сервер администрирования перейдите по ссылке Свойства Сервера администрирования.

Откроется окно Свойства: Сервер администрирования.

. В окне свойств Сервера администрирования в разделе Дополнительно выберите подраздел Информация об установленных плагинах управления программами.

В правой части окна в списке установленных плагинов управления отображается основной плагин управления Kaspersky Security: Kaspersky Kaspersky Security для виртуальных и облачных сред.

Если вы установили плагин управления Kaspersky Security для клиентов, также отображается Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов).

Запуск мастера первоначальной настройки управляемой программы

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

Если вы также установили плагин управления Kaspersky Security для клиентов, мастер первоначальной настройки управляемой программы запускается повторно и автоматически создает в папке Управляемые устройства главного Сервера администрирования политику для клиентов по умолчанию.

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

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

Чтобы запустить вручную мастер первоначальной настройки, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. В контекстном меню узла выберите пункт Все задачи → Мастер первоначальной настройки управляемой программы.

. Нажмите на кнопку Далее в окне приветствия.

. На следующем шаге выберите управляемую программу: Kaspersky Kaspersky Security для виртуальных и облачных сред и нажмите на кнопку Далее.

. Дождитесь окончания работы и закройте окно мастера.

. Если вы используете программу в режиме multitenancy, выполните повторно шаги 1–3, на следующем шаге выберите управляемую программу: Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) и нажмите на кнопку Далее.

. Дождитесь окончания работы и закройте окно мастера.

Политики и задачи по умолчанию

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

Основная политика по умолчанию

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

Параметры политики по умолчанию принимают следующие значения:

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

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

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

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

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

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

Политика для клиентов по умолчанию

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

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

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

Если вы хотите централизовано включить использование KSN для защиты всех виртуальных машин клиентов, вам нужно предварительно получить согласие клиентов на отправку в "Лабораторию Касперского" информации об использовании KSN, а также другой информации в зависимости от выбранного вами режима использования KSN (стандартный KSN или расширенный KSN).

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

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

В политике для клиентов по умолчанию вы можете настраивать параметры уведомлений о событиях, происходящих во время проверки и защиты виртуальных машин клиентов.

Задача обновления баз по умолчанию

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

Задача запускается при каждой загрузке пакета обновлений в хранилище Сервера администрирования Kaspersky Security Center и позволяет обновлять базы на всех SVM.

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

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

Параметры задачи полной проверки принимают следующие значения:

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

Вы можете запускать эту задачу вручную.

Настройка Сервера интеграции

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

Настройка параметров Сервера интеграции выполняется в Консоли Сервера интеграции.

Запуск Консоли Сервера интеграции

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

Чтобы запустить Консоль Сервера интеграции, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. Запустите Консоль Сервера интеграции по ссылке Управление Kaspersky Kaspersky Security для виртуальных и облачных сред на закладке Мониторинг в блоке Развертывание.

. Если выполняется одно из следующих условий, откроется окно для ввода параметров подключения к Серверу интеграции:

- если компьютер, на котором установлена Консоль Сервера интеграции, не входит в домен Active Directory;
- если компьютер, на котором установлена Консоль Сервера интеграции, входит в домен, но не удалось подключиться к Серверу интеграции, используя адрес и порт подключения, заданные в параметрах Консоли Сервера интеграции.

Укажите следующие параметры подключения:

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

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

Нажмите на кнопку Подключить.

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

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

Откроется Консоль Сервера интеграции.

Настройка параметров подключения Сервера интеграции к серверу управления виртуальной инфраструктурой

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

- для защиты виртуальной инфраструктуры под управлением одного или нескольких серверов VMware vCenter Server вам нужно настроить подключение Сервера интеграции к каждому из этих серверов VMware vCenter Server;

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

Подключение к каждому серверу управления виртуальной инфраструктурой выполняется отдельно.

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

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

. Запустите Консоль Сервера интеграции.

. В разделе Защита виртуальной инфраструктуры нажмите на кнопку Добавить.

. В открывшемся окне Подключение к виртуальной инфраструктуре выберите тип сервера управления виртуальной инфраструктурой, к которому требуется настроить подключение, и нажмите на кнопку Далее.

. Укажите следующие параметры:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) сервера управления виртуальной инфраструктурой, к которому подключается Сервер интеграции;

- имя и пароль учетной записи, под которой Сервер интеграции подключается к серверу управления виртуальной инфраструктурой.

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

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

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

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

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

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

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

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

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

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

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

. Разверните список возможных действий для выбранного сервера управления виртуальной инфраструктурой щелчком левой клавиши мыши по адресу или имени сервера управления виртуальной инфраструктурой в графе Адрес.

. В зависимости от типа сервера управления виртуальной инфраструктурой выберите действие Изменить параметры подключения к VMware vCenter Server или Изменить параметры подключения к VMware vCloud Director.
Откроется окно Подключение к виртуальной инфраструктуре.

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

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

. Разверните список возможных действий для выбранного сервера управления виртуальной инфраструктурой щелчком левой клавиши мыши по адресу или имени сервера управления виртуальной инфраструктурой в графе Адрес.

. В зависимости от типа сервера управления виртуальной инфраструктурой выберите действие Удалить VMware vCenter Server из списка или Удалить VMware vCloud Director из списка.

. Подтвердите удаление в открывшемся окне.

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

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

Изменение паролей учетных записей Сервера интеграции

Если требуется, в разделе Учетные записи Сервера интеграции вы можете изменить пароли учетных записей Сервера интеграции:

- Пароль учетной записи администратора Сервера интеграции (admin).
- Пароль учетной записи для подключения SVM к Серверу интеграции (svm).

  Пароль учетной записи svm требуется для настройки подключения SVM с установленным компонентом Защита от файловых угроз к Серверу интеграции, который будет осуществлять взаимодействие между сервером VMware vCenter Server и SVM.
- Пароль учетной записи для взаимодействия между VMware NSX Manager и Сервером интеграции (NSX_220E116BB6D5-42).

Имена учетных записей недоступны для изменения.

Чтобы изменить пароль учетной записи Сервера интеграции, выполните следующие действия:

. Запустите Консоль Сервера интеграции.

. В списке слева выберите раздел Учетные записи Сервера интеграции.

. Выберите в таблице имя учетной записи, пароль которой вы хотите изменить.

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

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

. Нажмите на кнопку ОК в окне Пароль учетной записи.

Просмотр параметров Сервера интеграции

Чтобы просмотреть параметры Сервера интеграции, выполните следующие действия:

. Запустите Консоль Сервера интеграции.

. В списке слева выберите раздел Параметры Сервера интеграции.

В правой части Консоли отображаются следующие параметры Сервера интеграции, к которому выполнено подключение:

- Версия Сервера интеграции.
- Имя учетной записи, под которой выполнено подключение к Серверу интеграции.
- Тип аутентификации, который использовался при подключении к Серверу интеграции.
- IP-адрес в формате IPv4 или полное доменное имя (FQDN) и порт Сервера интеграции.

Если вы включили запись информации в файл трассировки Сервера интеграции, вы можете открыть для просмотра этот файл по ссылке Посмотреть файл трассировки. Файл трассировки открывается в текстовом редакторе Блокнот.

Регистрация служб Kaspersky Security

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

- регистрации в VMware NSX Manager служб Kaspersky Security: службы защиты файловой системы (Kaspersky File Antimalware Protection) и службы сетевой защиты (Kaspersky Network Protection); развертывания служб Kaspersky Security;
- первоначальной настройки конфигурации новых SVM после развертывания служб Kaspersky Security.
- Регистрацию служб Kaspersky Security в VMware NSX Manager и настройку конфигурации новых SVM выполняет Сервер интеграции.

Чтобы ввести параметры, необходимые для регистрации и развертывания служб Kaspersky Security, выполните следующие действия:

. Запустите Консоль Сервера интеграции.

Откроется раздел Защита виртуальной инфраструктуры.

. В списке выберите сервер VMware vCenter Server и разверните список доступных действий щелчком левой клавиши мыши по адресу или имени VMware vCenter Server в графе Адрес.

. В блоке Управление защитой выберите действие Зарегистрировать службы Kaspersky Security.

Запустится мастер регистрации служб Kaspersky Security. Следуйте указаниям мастера.

Подключение к VMware NSX Manager

На этом шаге укажите параметры подключения Сервера интеграции к VMware NSX Manager: IP-адрес в

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

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

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

Перейдите к следующему шагу мастера.

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

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

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

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

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

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

Выбор образа SVM для службы защиты файловой системы

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

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

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

Чтобы указать образ SVM, выполните следующие действия:

. Укажите в поле адрес файла описания образов SVM (файла в формате XML) или адрес OVF-файла образа SVM, соответствующего нужной конфигурации SVM.

. Нажмите на кнопку Проверить.

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

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

- Конфигурация SVM – количество выделенных для SVM процессоров и оперативной памяти.
  Если вы указали адрес файла описания образов SVM (файла в формате XML), вы можете выбрать нужную конфигурацию SVM в раскрывающемся списке в поле Конфигурация SVM.
- Название программы – название программы, которая установлена на SVM.
- Версия SVM – номер версии SVM.
- Производитель – производитель программы, которая установлена на SVM.
- Описание – краткое описание программы.
- Необходимое место на диске – объем дискового пространства, которое требуется для развертывания SVM в хранилище данных.

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

Перейдите к следующему шагу мастера.

Выбор образа SVM для службы сетевой защиты

Если вы хотите установить компонент Защита от сетевых угроз, на этом шаге укажите образ SVM с установленным компонентом Защита от сетевых угроз. Сервер интеграции зарегистрирует службу сетевой защиты (Kaspersky Network Protection) в VMware NSX Manager. После завершения регистрации вы можете выполнить развертывание службы сетевой защиты на кластерах VMware. В результате на гипервизорах будут развернуты SVM с компонентом Защита от сетевых угроз.

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

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

Чтобы указать образ SVM, выполните следующие действия:

. Укажите в поле адрес файла описания образов SVM (файла в формате XML) или адрес OVF-файла образа SVM, соответствующего нужной конфигурации SVM.

. Нажмите на кнопку Проверить.

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

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

- Конфигурация SVM – количество выделенных для SVM процессоров и оперативной памяти.
  Если вы указали адрес файла описания образов SVM (файла в формате XML), вы можете выбрать нужную конфигурацию SVM в раскрывающемся списке в поле Конфигурация SVM.
- Название программы – название программы, которая установлена на SVM.
- Версия SVM – номер версии SVM.
- Производитель – производитель программы, которая установлена на SVM.
- Описание – краткое описание программы.
- Необходимое место на диске – объем дискового пространства, которое требуется для развертывания SVM в хранилище данных.

Если вы не хотите устанавливать компонент Защита от сетевых угроз, снимите флажок Зарегистрировать службу сетевой защиты.

Перейдите к следующему шагу мастера.

Выбор режима обработки трафика для компонента Защита от сетевых угроз

Если на предыдущем шаге вы указали образ SVM с установленным компонентом Защита от сетевых угроз, на этом шаге вам нужно выбрать режим обработки трафика для компонента Защита от сетевых угроз. Режим обработки трафика определяет параметры работы программы, установленной на SVM с компонентом Защита от сетевых угроз.

Вы можете выбрать один из следующих режимов обработки трафика:

- Стандартный режим. Если выбран этот режим, виртуальный фильтр (VMware DVFilter) перехватывает трафик виртуальных машин и передает на проверку программе Kaspersky Security. При обнаружении признаков вторжений или попытки доступа

к опасным или нежелательным веб-адресам Kaspersky Security выполняет то действие, которое указано в параметрах политики, и передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

Этот вариант выбран по умолчанию.

- Режим мониторинга. Если выбран этот режим, программа Kaspersky Security получает копию трафика виртуальных машин. При обнаружении признаков вторжений или попытки доступа к опасным или нежелательным веб-адресам Kaspersky Security не предпринимает действий по предотвращению угроз, а только передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

После регистрации службы сетевой защиты и развертывания SVM изменить режим обработки трафика невозможно. Чтобы выбрать другой режим обработки трафика, вам потребуется удалить SVM, отменить регистрацию службы сетевой защиты, а затем повторно выполнить регистрацию службы сетевой защиты с новым режимом обработки трафика и развернуть новые SVM.

Перейдите к следующему шагу мастера.

Настройка параметров подключений для SVM

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

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

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

Перейдите к следующему шагу мастера.

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

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

Создание паролей учетных записей на SVM

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

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

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

После развертывания SVM для предотвращения несанкционированного доступа к SVM рекомендуется регулярно изменять пароль конфигурирования. Вы можете изменить пароль конфигурирования с помощью процедуры изменения параметров Kaspersky Security.

Перейдите к следующему шагу мастера.

Выбор часового пояса для SVM

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

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

Перейдите к следующему шагу мастера.

Настройка параметров подключения к сетевому хранилищу данных

На этом шаге вы можете настроить следующие параметры использования сетевого хранилища данных:

- разрешить или запретить использование сетевого хранилища данных для SVM; указать
- параметры подключения SVM к сетевому хранилищу данных.

Сетевое хранилище данных может использоваться для хранения резервных копий файлов, помещенных в резервные хранилища на SVM. По умолчанию SVM не используют сетевое хранилище данных.

Если вы хотите разрешить использование сетевого хранилища данных для SVM, выберите вариант Использовать сетевое хранилище данных и укажите следующие параметры подключения к хранилищу:

- Адрес сетевого хранилища данных в формате UNC.

  В качестве адреса не может быть указано localhost или 127.0.0.1.

- Учетную запись, с которой SVM должны подключаться к сетевому хранилищу данных, в виде <домен>\<имя пользователя>.
- Пароль учетной записи для подключения.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к сетевому хранилищу данных с указанными параметрами.

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

Подтверждение параметров Kaspersky Security

На этом шаге проверьте введенные параметры Kaspersky Security.

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

Процесс регистрации служб Kaspersky Security

На этом шаге отображается информация о действиях, которые выполняет Сервер интеграции, чтобы зарегистрировать службы 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.

Завершение работы мастера

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

Если регистрация служб завершилась успешно, завершите работу мастера.

Если регистрация служб 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 файлах трассировки Сервера интеграции (если вы включили запись информации в файлы трассировки Сервера интеграции).

Просмотр зарегистрированных служб в консоли VMware vSphere Web Client

Регистрацию служб 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 .

Развертывание SVM с компонентами Защита от файловых угроз и Защита от сетевых угроз

Чтобы развернуть SVM с компонентами Kaspersky Security на гипервизорах VMware ESXi, вам нужно развернуть службы Kaspersky Security на кластерах VMware. Развертывание служб Kaspersky Security выполняется в консоли VMware vSphere Web Client.

Чтобы развернуть SVM с компонентами Kaspersky Security, выполните следующие действия:

. В консоли VMware vSphere Web Client запустите мастер развертывания сетевых служб и служб обеспечения защиты виртуальных машин (раздел Networking & Security → Installation and Upgrade закладка Service Deployments).

. С помощью мастера укажите следующие параметры:

a. Выберите в таблице службу, которую требуется развернуть:

- службу Kaspersky File Antimalware Protection, если вы хотите развернуть SVM с компонентом Защита от файловых угроз;
- службу Kaspersky Network Protection, если вы хотите развернуть SVM с компонентом Защита от сетевых угроз.

Вы можете выбрать обе службы Kaspersky Security, если требуется развернуть SVM с компонентом Защита от файловых угроз и SVM с компонентом Защита от сетевых угроз на одних и тех же гипервизорах и назначить им одинаковые параметры. Если параметры SVM или гипервизоры, на которых должны быть развернуты SVM, должны отличаться, вам нужно выполнить развертывание служб Kaspersky Security по отдельности.

b. Выберите один или несколько кластеров VMware, на которых вы хотите развернуть SVM с компонентами Kaspersky Security.

c. Если требуется, измените заданные по умолчанию параметры для всех SVM, которые будут развернуты на гипервизорах в составе каждого 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.

. Завершите работу мастера и дождитесь завершения развертывания служб Kaspersky Security.

SVM с компонентом Защита от файловых угроз и SVM с компонентом Защита от сетевых угроз будут развернуты на каждом гипервизоре в составе каждого кластера VMware, который вы выбрали.

Подробнее о процедуре развертывания SVM с компонентами Kaspersky Security см. в Базе знаний .

Настройка групп безопасности NSX (NSX Security Group)

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

Чтобы настроить группу безопасности NSX, выполните следующие действия:

. В консоли VMware vSphere Web Client запустите мастер создания группы безопасности NSX в разделе Networking & Security → Service Composer на закладке Security Groups.

. С помощью мастера введите название новой группы безопасности NSX (например, "Kaspersky Security Group" или "Protected by Kaspersky") и настройте правила включения виртуальных машин в группу.

Предусмотрены следующие способы включения виртуальных машин в группу безопасности NSX:

- Динамическое включение виртуальных машин в группу безопасности NSX. В группу входят все виртуальные машины, которые удовлетворяют указанным критериям.

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

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

Подробнее о настройке групп безопасности NSX см. в Базе знаний .

Настройка и применение политик безопасности NSX (NSX Security Policy)

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

В каждой политике безопасности NSX вам требуется настроить использование служб Kaspersky Security:

- службы защиты файловой системы (Kaspersky File Antimalware Protection), если вы хотите защищать виртуальные машины от файловых угроз;

- службы сетевой защиты (Kaspersky Network Protection), если вы хотите защищать виртуальные машины от сетевых угроз.

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

. В консоли VMware vSphere Web Client запустите мастер создания политики безопасности NSX в разделе Networking & Security → Service Composer на закладке Security Policies.

. Если вы хотите защищать виртуальные машины от файловых угроз, на шаге мастера Guest Introspection Services добавьте службу Kaspersky File Antimalware Protection с произвольным названием и действием по умолчанию (Apply).

. Если вы хотите проверять исходящий трафик виртуальных машин, на шаге мастера Network Introspection Services добавьте службу Kaspersky Network Protection и укажите для нее следующие значения параметров:

- Произвольное название.
- Перенаправление трафика службе сетевой защиты (Kaspersky Network Protection) – включено (параметр Redirect to service).
- Source – Policy's Security Groups (установлено по умолчанию).
- Destination – Any (установлено по умолчанию).

. Если вы хотите проверять входящий трафик виртуальных машин, на шаге мастера Network Introspection Services добавьте службу Kaspersky Network Protection и укажите для нее следующие значения параметров:

- Произвольное название.
- Перенаправление трафика службе сетевой защиты (Kaspersky Network Protection) – включено (параметр Redirect to service).
- Source – Any.
- Destination – Policy's Security Groups.

. Завершите работу мастера создания политики безопасности NSX.

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

Подробнее о настройке политик безопасности NSX см. в Базе знаний.

Настройка защиты организаций-клиентов

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

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

. В Консоли администрирования Kaspersky Security Center для каждого клиента, виртуальные машины которого требуется защищать, создать виртуальный Сервер администрирования и учетную запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования.

. В Консоли администрирования Kaspersky Security Center создать учетную запись, под которой Сервер интеграции будет подключаться к Серверу администрирования Kaspersky Security Center. Подключение требуется для получения информации о виртуальных Серверах администрирования, созданных в Kaspersky Security Center, и для настройки соответствий между виртуальными Серверами администрирования и организациями vCloud Director, которые содержат виртуальные машины клиентов.

. В Консоли Сервера интеграции выполнить подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center и настроить список соответствий между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center.

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

. Передать администратору клиента следующую информацию:

- адрес Сервера интеграции; адрес виртуального Сервера администрирования, настроенного для этого
- клиента; имя и пароль учетной записи для подключения к виртуальному Серверу администрирования.

. Убедиться в том, что программа подготовлена к работе и настроены политики для защиты виртуальной инфраструктуры каждого клиента:

- для защиты от файловых угроз на каждом виртуальном Сервере администрирования Kaspersky Security Center, соответствующем организации-клиенту, должна быть настроена политика для клиентов;
- для защиты от сетевых угроз должна быть настроена основная политика, в области действия которой находятся виртуальные машины клиента.

Создание виртуального Сервера администрирования для клиента

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

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

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

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

. В Консоли администрирования Kaspersky Security Center в папке Управляемые устройства выберите группу администрирования, которая содержит кластер "VMware vCloud Director Agentless", затем выберите вложенную папку Серверы администрирования.

. В рабочей области папки Серверы администрирования перейдите по ссылке Добавить виртуальный Сервер администрирования.

Запустится мастер добавления виртуального Сервера администрирования.

. На первом шаге мастера укажите имя создаваемого виртуального Сервера администрирования.

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

Перейдите к следующему шагу мастера.

. Укажите адрес Сервера администрирования Kaspersky Security Center, на котором создается виртуальный Сервер администрирования, и перейдите к следующему шагу мастера.

. Укажите учетную запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования. Вы можете указать ранее созданную учетную запись внутреннего пользователя Kaspersky Security Center или создать учетную запись с помощью кнопки Создать.

Перейдите к следующему шагу мастера.

. Запустите создание виртуального Сервера администрирования с помощью кнопки Далее.

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

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

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

Подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center

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

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

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

. Запустите Консоль Сервера интеграции.

. В списке слева выберите раздел Управление защитой организаций-клиентов.

. В блоке Параметры подключения к Kaspersky Security Center укажите параметры подключения:

- IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера администрирования Kaspersky Security Center.
- Имя и пароль учетной записи, под которой Сервер интеграции должен подключаться к Серверу администрирования Kaspersky Security Center.

. Нажмите на кнопку Подключить. Статус подключения Сервера интеграции к Серверу администрирования Kaspersky Security Center отображается в блоке Статус подключения к Kaspersky Security Center в верхней части окна.

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

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

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

Настройка списка соответствий между организациями vCloud Director и виртуальными Серверами администрирования

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

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

- устанавливать соответствия между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center; просматривать список установленных соответствий;
- отменять установленные соответствия.

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

. Запустите Консоль Сервера интеграции.

. В списке слева выберите раздел Управление защитой организаций-клиентов и убедитесь, что Сервер интеграции подключен к Серверу администрирования Kaspersky Security Center. Выполните подключение, если подключение не установлено.

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

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

- В разделе Защита виртуальной инфраструктуры разверните список доступных действий для сервера VMware vCloud Director, под управлением которого находится организация vCloud Director, и перейдите по ссылке Установить соответствия для организаций vCloud Director. Откроется список соответствий для организаций vCloud Director, которые находятся под управлением одного сервера VMware vCloud Director.

- В разделе Управление защитой организаций-клиентов нажмите на кнопку Открыть список, расположенную в блоке Список соответствий между организациями vCloud Director и виртуальными Серверами администрирования. Откроется список соответствий для организаций vCloud Director, которые находятся под управлением всех серверов VMware vCloud Director.

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

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

- Виртуальный Сервер – имя виртуального Сервера администрирования, которому соответствует организация из графы Организация vCloud Director. Если соответствие с организацией vCloud Director для этого виртуального Сервера администрирования не установлено, в графе отображается значение нет.

- Организация vCloud Director – имя организации vCloud Director, которой соответствует виртуальный Сервер администрирования из графы Виртуальный Сервер. Если соответствие с виртуальным Сервером администрирования для этой организации vCloud Director не установлено, в графе отображается значение нет.

- VMware vCloud Director – IP-адрес или имя сервера VMware vCloud Director, под управлением которого находится организация из графы Организация vCloud Director. Если организация vCloud Director в этой строке таблицы не указана, в графе отображается значение нет.

При просмотре списка соответствий вы можете использовать следующие возможности:

- Фильтр. Чтобы применить фильтр, вы можете использовать следующие ссылки, расположенные над таблицей: Все –

- показывать в таблице все строки. Это значение выбрано по умолчанию.

- Соответствие установлено – показывать только строки, в которых отображается имя организации vCloud Director и имя виртуального Сервера администрирования, между которыми установлено соответствие.

- Соответствие не установлено – показывать только строки, в которых отображается имя организации vCloud Director или имя виртуального Сервера администрирования, для которых соответствия не установлены.

- Поиск по любой графе таблицы. Вы можете ввести условие поиска в поисковой строке, расположенной над таблицей, чтобы найти организацию vCloud Director, виртуальный Сервер администрирования или сервер VMware vCloud Director. Поиск инициируется во время ввода символов. В таблице отображаются все строки, в которых присутствует значение, удовлетворяющее условиям поиска. Чтобы сбросить результаты поиска, нужно удалить содержимое строки поиска.

Установка соответствия между организацией vCloud Director и виртуальным Сервером администрирования

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

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

. Запустите Консоль Сервера интеграции.

. Выберите раздел Управление защитой организаций-клиентов и убедитесь, что Сервер интеграции подключен к Серверу администрирования Kaspersky Security Center. Выполните подключение, если подключение не установлено.

. Откройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования.

. Выполните одно из следующих действий:

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

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

Для поиска нужной строки в таблице вы можете использовать фильтр или поисковую строку.

. В открывшемся окне выберите виртуальный Сервер администрирования или организацию vCloud Director и нажмите на кнопку ОК.

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

Отмена соответствия между организацией vCloud Director и виртуальным Сервером администрирования

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

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

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

. Запустите Консоль Сервера интеграции.

. Откройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования.

. Найдите в таблице строку, которая содержит организацию vCloud Director и виртуальный Сервер администрирования, соответствие между которыми вы хотите отменить.

Для поиска нужной строки в таблице вы можете использовать фильтр или поисковую строку.

. Нажмите на значок  , расположенный в строке, и подтвердите отмену соответствия в открывшемся окне.

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

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

Подготовка программы к работе и первоначальная настройка

После установки программы требуется подготовить программу к работе. Для этого нужно выполнить следующие действия:

- Активировать программу на всех новых SVM.
- Обновить базы программы на всех новых SVM.
- Включить защиту виртуальных машин от файловых и сетевых угроз. По умолчанию Kaspersky Security не защищает виртуальные машины.

Активация программы на новых SVM

Чтобы активировать программу, требуется добавить лицензионный ключ на все SVM. 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 с операционными системами для рабочих станций и с операционными системами для серверов вам нужно создать две задачи активации: для добавления ключа для серверов на SVM и для добавления ключа для рабочих станций на SVM.

Чтобы настроить задачу активации, выполните следующие действия:

. Добавьте лицензионный ключ в хранилище ключей Kaspersky Security Center.

. В дереве Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача. Запустится мастер создания задачи.

. Укажите программу, для которой создается задача, и тип задачи. Для этого в списке Kaspersky Kaspersky Security для виртуальных и облачных сред выберите Активация программы.

Перейдите к следующему шагу мастера.

. Нажмите на кнопку Выбрать. Откроется окно Выбор ключа. Выберите ключ из хранилища ключей Kaspersky Security Center и нажмите на кнопку ОК.

Перейдите к следующему шагу мастера.

. Настройте параметры расписания запуска задачи:

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

Перейдите к следующему шагу мастера.

. Введите название задачи и перейдите к следующему шагу мастера.

. Завершите работу мастера.

В соответствии с настроенными параметрами расписания 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.

Обновление баз программы на новых SVM

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

Чтобы обновить базы программы после установки или обновления программы, выполните следующие действия:

. Убедитесь в том, 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).

. Запустите вручную задачу загрузки обновлений в хранилище или дождитесь запуска задачи по расписанию. Убедитесь в том, что задача загрузки обновлений в хранилище выполнена успешно (см. подробнее в документации Kaspersky Security Center).

. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы.

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

Если задача обновления баз программы отсутствует, создайте ее.

. Дождитесь запуска по расписанию задачи обновления баз программы или запустите задачу вручную.

. Убедитесь в том, что задача обновления баз программы выполнена успешно.

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

Включение защиты виртуальных машин

По умолчанию Kaspersky Security не защищает виртуальные машины. После установки программы Kaspersky Security нужно включить защиту виртуальных машин с помощью политики.

Для защиты от файловых угроз виртуальных машин, которые не входят в состав организаций vCloud Director, вы можете использовать основную политику по умолчанию или создать основную политику.

Если программа работает в режиме multitenancy, для защиты виртуальной инфраструктуры клиентов от файловых угроз требуется создать политику для клиентов на каждом виртуальном Сервере администрирования Kaspersky Security Center, соответствующем организации-клиенту. Создать политику для клиентов может администратор провайдера или администратор клиента. Параметры

защиты виртуальной инфраструктуры клиентов от сетевых угроз будут определяться основной политикой, в области действия которой находятся виртуальные машины клиента.

Защита от файловых угроз

Чтобы защищать виртуальную машину от файловых угроз, нужно назначить виртуальной машине профиль защиты. Виртуальная машина, которой не назначен профиль защиты, исключается из защиты.

Профиль защиты может назначаться непосредственно объектам виртуальной инфраструктуры (включая виртуальные машины) или путем установки соответствия между профилем защиты и конфигурацией профиля NSX (NSX Profile Configuration), действие которой распространяется на виртуальные машины.

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

Kaspersky Security защищает только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин от файловых угроз.

Защита от сетевых угроз

Чтобы защищать виртуальную машину от сетевых угроз, нужно настроить параметры предотвращения вторжений и / или проверки веб-адресов в свойствах политики, в области действия которой находится виртуальная машина.

Kaspersky Security защищает только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин от сетевых угроз.

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

Создание основной политики

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

Чтобы создать основную политику, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center запустите мастер создания политики:

a. В дереве консоли выберите папку или группу администрирования, в которой вы хотите создать политику.

b. В рабочей области выберите закладку Политики и нажмите на кнопку Новая политика.

. На первом шаге мастера создания политики в списке выберите Kaspersky Kaspersky Security для виртуальных и облачных сред и перейдите к следующему шагу мастера.

. Введите название новой политики и перейдите к следующему шагу мастера.

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

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

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

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

Перейдите к следующему шагу мастера создания политики.

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

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

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

- Если вы создаете политику в группе администрирования, которая содержит кластер "VMware vCenter

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

Agentless", выберите вариант Один сервер VMware vCenter Server. Затем выберите в списке VMware vCenter Server, соответствующий этому кластеру KSC.

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

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

Нажмите на кнопку ОК в окне Выбор защищаемой инфраструктуры.

. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты.

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

Перейдите к следующему шагу мастера.

. На этом шаге вы можете включить SNMP-мониторинг состояния SVM.

Чтобы предотвратить несанкционированный доступ к службе SNMP, вы можете сформировать список IPадресов, на которые агент SNMP должен передавать информацию о состоянии SVM.
Перейдите к следующему шагу мастера.

. Примите решение об участии в Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

- Если вы хотите использовать KSN в работе программы и согласны со всеми пунктами Положения, выберите вариант Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network.

- Если вы не хотите принимать участие в KSN, выберите вариант Я не принимаю условия настоящего Положения о Kaspersky Security Network и подтвердите свое решение в открывшемся окне.

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

Если вы хотите использовать KSN в работе Kaspersky Security, убедитесь в том, что использование KSN нужного вам типа настроено в Kaspersky Security Center. Для использования Глобального KSN в Kaspersky Security Center должна быть включена служба прокси-сервера KSN. Для использования Локального KSN требуется включить и настроить использование Локального KSN в Kaspersky Security Center. См. подробнее в документации Kaspersky Security Center.

При необходимости позже вы сможете изменить параметры использования KSN в работе программы.

Перейдите к следующему шагу мастера.

. Завершите работу мастера создания политики.

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

После создания политики вы можете назначить профили защиты виртуальным машинам, которые вы хотите защищать.

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

Сетевая защита по умолчанию выключена во всех политиках. Вы можете настроить параметры защиты от сетевых угроз в свойствах политики.

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

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

Создание политики для клиентов

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

Чтобы создать политику для клиентов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center запустите мастер создания политики:

a. В дереве консоли выберите папку или группу администрирования, в которой вы хотите создать политику.

b. В рабочей области выберите закладку Политики и нажмите на кнопку Новая политика.

. На первом шаге мастера в списке выберите Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) и перейдите к следующему шагу мастера.

. Введите название новой политики и перейдите к следующему шагу мастера.

. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера.

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

Мастер проверяет SSL-сертификат, полученный от Сервера интеграции. Если полученный сертификат содержит ошибку, откроется окно Проверка сертификата с сообщением об ошибке. SSL-сертификат используется для установки защищенного

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

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

. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты.

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

Перейдите к следующему шагу мастера.

. Примите решение об участии в Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

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

При необходимости позже вы сможете изменить свое решение.

Параметры использования KSN (тип и режим использования KSN) определяются основной политикой, в области действия которой находятся виртуальные машины клиента.

Перейдите к следующему шагу мастера.

. Завершите работу мастера создания политики.

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

В политике для клиентов, которая расположена в папке Управляемые устройства виртуального Сервера администрирования, по умолчанию включена файловая защита (используется основной профиль защиты). Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе защищаемой инфраструктуры, вам нужно создать и назначить дополнительные профили защиты в свойствах политики.

В политике для клиентов, которая расположена в папке Управляемые устройства главного Сервера

администрирования или в группе администрирования, которая содержит кластер "VMware vCloud Director Agentless", файловая защита по умолчанию выключена.

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

Обновление предыдущей версии программы

Вы можете обновить до версии Kaspersky Kaspersky Security для виртуальных и облачных сред следующие версии программы:

- Kaspersky Security для виртуальных сред 5.0 Защита без агента.
- Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента.
- Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Защита без агента.
- Kaspersky Security для виртуальных сред 4.0 Защита без агента.

Перед началом обновления программы вам нужно выполнить следующие действия:

- Загрузить с веб-сайта "Лаборатории Касперского" все файлы образов SVM. О способах проверки подлинности образа SVM см. на странице программы в Базе знаний.
- Разместить все файлы образов SVM в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS. Например, вы можете опубликовать образы SVM на Веб-сервере Kaspersky Security Center.
- Убедиться в том, что в настройках сетевого оборудования или программного обеспечения, используемого для контроля трафика, открыты порты, которые требуются для работы программы.
- Убедиться в том, что настроены параметры учетных записей, которые требуются для установки и работы программы.
- Если вы планируете использовать сетевое хранилище данных для SVM, создать сетевую папку для размещения сетевого хранилища данных и учетную запись для подключения SVM. Сетевое хранилище данных используется для хранения резервных копий файлов, помещенных в резервные хранилища на SVM. Место, которое требуется для сетевого хранилища данных, можно оценить по формуле: (N+1) ГБ, где N – количество SVM, которые подключаются к сетевому хранилищу данных.

Процедура обновления программы зависит от типа инфраструктуры, в которой была установлена программа предыдущей версии. Предусмотрены следующие варианты обновления программы:

- Обновление программы, установленной в инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager.
- Обновление программы, установленной в инфраструктуре под управлением VMware vCenter Server и VMware vShield Manager, с переходом на платформу VMware NSX.

Обновление программы, установленной в инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager

Перед началом обновления программы рекомендуется убедиться, что виртуальная инфраструктура VMware соответствует программным требованиям Kaspersky Security. Если в состав кластеров VMware, которые защищает Kaspersky Security, входят гипервизоры VMware ESXi 5.5, пред началом обновления программы требуется выполнить следующие действия:

. Для всех кластеров VMware, в состав которых входит один или несколько гипервизоров VMware ESXi 5.5, удалить развернутые службы Kaspersky Security. Удаление выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Installation and Upgrade на закладке Service Deployments).

. Обновить все гипервизоры VMware ESXi 5.5 для соответствия программным требованиям Kaspersky Security или удалить все гипервизоры VMware ESXi 5.5 из состава кластеров VMware, которые вы хотите защищать с помощью программы Kaspersky Security.

Обновление состоит из следующих этапов:

. Обновление Kaspersky Security Center. Для работы программы Kaspersky Kaspersky Security для виртуальных и облачных сред требуется обновить Kaspersky Security Center до одной из следующих версий:

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

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

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

Подробнее об обновлении Kaspersky Security Center см. в документации Kaspersky Security Center.

. Установка новой версии плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции.

Если вы хотите использовать программу в режиме multitenancy, вам нужно также установить плагин управления Kaspersky Security для клиентов.

. Обновление SVM с компонентами программы Kaspersky Security в виртуальной инфраструктуре.

Если вы хотите использовать программу в режиме multitenancy, рекомендуется настроить параметры подключения Сервера интеграции к серверу VMware vCloud Director перед обновлением SVM.

При обновлении SVM с компонентом Защита от файловых угроз автоматически удаляются копии файлов, помещенные в резервное хранилище.

. Конвертация политик и задач предыдущей версии программы. Если вы обновляете программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента или ниже, вам нужно выполнить конвертацию с помощью мастера.

Если вы обновляете программу версии Kaspersky Security для виртуальных сред 5.0 Защита без агента, политики и задачи конвертируются автоматически в политики и задачи Kaspersky Kaspersky Security для виртуальных и облачных сред после первого изменения и сохранения параметров защиты в политике и параметров проверки в задаче.

После завершения обновления рекомендуется убедиться в том, что на новых SVM программа подготовлена к работе.

Если вы хотите использовать программу в режиме multitenancy, после установки программы вам нужно настроить защиту организаций-клиентов.

Обновление программы, установленной в инфраструктуре под управлением VMware vCenter Server и VMware vShield Manager, с переходом на платформу VMware NSX

Обновление состоит из следующих этапов:

. Удаление компонента Защита от файловых угроз и компонента Защита от сетевых угроз предыдущей версии программы. Порядок удаления компонентов см. в документации Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Защита без агента или Kaspersky Security для виртуальных сред 4.0 Защита без агента .

При удалении SVM с компонентом Защита от файловых угроз автоматически удаляются копии файлов, помещенные в резервное хранилище.

. Обновление виртуальной инфраструктуры VMware для соответствия программным требованиям Kaspersky Security. В виртуальной инфраструктуре требуется удалить VMware vShield Manager и развернуть VMware NSX for vSphere 6.3.7 или VMware NSX for vSphere 6.4.6. В инфраструктуре под управлением VMware vCenter Server и VMware vShield Manager работа компонентов Kaspersky Kaspersky Security для виртуальных и облачных сред не поддерживается.

. Подготовка виртуальной инфраструктуры к установке компонентов Kaspersky Security.

. Обновление Kaspersky Security Center. Для работы программы Kaspersky Kaspersky Security для виртуальных и облачных сред требуется обновить Kaspersky Security Center до одной из следующих версий:

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

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

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

Подробнее об обновлении Kaspersky Security Center см. в документации Kaspersky Security Center.

. Установка новой версии плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции.

Если вы хотите использовать программу в режиме multitenancy, вам нужно также установить плагин управления Kaspersky Security для клиентов.

. Настройка параметров подключения Сервера интеграции к одному или нескольким серверам управления виртуальной инфраструктурой.

. Регистрация в VMware NSX Manager служб Kaspersky Security.

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

Если вы хотите установить компонент Защита от сетевых угроз, вам нужно зарегистрировать службу сетевой защиты (Kaspersky Network Protection).

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

В консоли VMware vSphere Web Client вы можете убедиться в том, что регистрация служб Kaspersky Security завершилась успешно.

. Развертывание SVM с компонентом Защита от файловых угроз и SVM с компонентом Защита от сетевых угроз на гипервизорах VMware ESXi. Развертывание SVM выполняется в консоли VMware vSphere Web Client.

После развертывания SVM Сервер интеграции передает на каждую новую SVM параметры конфигурации, которые вы указали при регистрации служб Kaspersky Security.

Развернутые SVM объединяются в кластеры KSC.

Если вы обновляете программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента, Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Защита без агента или Kaspersky Security для виртуальных сред 4.0 Защита без агента, в Консоли администрирования Kaspersky Security Center также отображаются группы администрирования, созданные для кластеров KSC предыдущей версией программы Kaspersky Security.

Кластер KSC для SVM предыдущей версии программы и созданная для него группа администрирования имеют название VMware vCenter "<имя>" (<IP-адрес>), где:

- <имя> – имя сервера VMware vCenter Server, соответствующего кластеру KSC для предыдущей версии программы. Если имя VMware vCenter Server не задано или совпадает с его IP-адресом, то имя опускается.

- <IP-адрес> – IP-адрес сервера VMware vCenter Server, соответствующего кластеру KSC для предыдущей версии программы.

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

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

a. Включить виртуальные машины в одну или несколько групп безопасности NSX (NSX Security Group).

b. Настроить одну или несколько политик безопасности NSX (NSX Security Policy) и применить политики безопасности на группы безопасности NSX.

. Конвертация политик и задач предыдущей версии программы. Если вы обновляете программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента или ниже, вам нужно выполнить конвертацию с помощью мастера.

Если вы обновляете программу версии Kaspersky Security для виртуальных сред 5.0 Защита без агента, политики и задачи конвертируются автоматически в политики и задачи Kaspersky Kaspersky Security для виртуальных и облачных сред после первого изменения и сохранения параметров защиты в политике и параметров проверки в задаче.

. Подготовка программы к работе на всех SVM.

Если вы хотите использовать программу в режиме multitenancy, после обновления программы вам нужно настроить защиту организаций-клиентов.

Об установке новой версии плагина управления Kaspersky Security и Сервера интеграции

Независимо от выбранного варианта использования программы вам нужно установить основной плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции.

Если вы хотите использовать программу в режиме multitenancy, вам нужно также установить плагин управления Kaspersky Security для клиентов.

При первом запуске Консоли администрирования Kaspersky Security Center после установки плагинов управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. Мастер позволяет создать политики по умолчанию и задачи.

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

Плагин управления предыдущей версии программы удалять не требуется, он удаляется автоматически.

Обновление SVM

Если вы хотите использовать программу в режиме multitenancy, рекомендуется настроить параметры подключения Сервера интеграции к серверу VMware vCloud Director перед обновлением SVM. Если вы подключаете Сервер интеграции к VMware vCloud Director после обновления SVM, для обеспечения правильной работы программы вам нужно выполнить дополнительные действия, описанные в Базе знаний.

Чтобы обновить SVM с компонентами программы Kaspersky Security в виртуальной инфраструктуре, выполните следующие действия:

. Для каждого сервера VMware vCenter Server, под управлением которого работают SVM с предыдущей версией программы, выполните процедуру изменения параметров Kaspersky Security. В ходе выполнения процедуры укажите адреса образов SVM с новой версией компонентов Kaspersky Security.

После завершения работы мастера изменения параметров Сервер интеграции повторно зарегистрирует службы Kaspersky Security с новыми параметрами.

. В консоли VMware vSphere Web Client выполните одно из следующих действий:

- Если в состав кластера VMware входили гипервизоры VMware ESXi 5.5 и перед началом обновления программы вы удалили развернутые службы Kaspersky Security, разверните службы Kaspersky Security на кластере.
- Если в состав кластера VMware не входили гипервизоры VMware ESXi 5.5, обновите на кластере развернутые службы Kaspersky Security (раздел Networking & Security → Installation and Upgrade, закладка Service Deployments, действие Upgrade).

Если вы обновляете программу версии Kaspersky Security для виртуальных сред 5.0 Защита без агента, новые SVM размещаются в тех же кластерах "VMware vCenter Agentless", в которых находились SVM с предыдущей версией программы.

Если вы обновляете программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента, Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Защита без агента или Kaspersky Security для виртуальных сред 4.0 Защита без агента, Kaspersky Security Center создает для новых SVM новые кластеры "VMware vCenter Agentless". В Консоли администрирования Kaspersky Security Center также отображаются группы администрирования, созданные для кластеров KSC предыдущей версии программы Kaspersky Security.

Кластер KSC для SVM предыдущей версии программы и созданная для него группа администрирования имеют название VMware vCenter "<имя>" (<IP-адрес>), где:

- <имя> – имя сервера VMware vCenter Server, соответствующего кластеру KSC для предыдущей версии программы. Если имя VMware vCenter Server не задано или совпадает с его IP-адресом, то имя опускается. • <IP-адрес> – IP-адрес сервера VMware vCenter Server, соответствующего кластеру KSC для предыдущей версии программы.

Конвертация политик и задач

После обновления программы вы можете использовать настроенные политики и задачи предыдущей версии программы Kaspersky Security.

Если вы обновили программу версии Kaspersky Security для виртуальных сред 5.0 Защита без агента, политики и задачи конвертируются автоматически в политики и задачи Kaspersky Kaspersky Security для виртуальных и облачных сред после первого изменения и сохранения параметров защиты в политике и параметров проверки в задаче.

Если вы обновили программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента или ниже, вам нужно выполнить следующие действия:

. Сконвертировать политики и задачи с помощью мастера массовой конвертации политик и задач Kaspersky Security Center.

Вы можете сконвертировать политики и задачи, настроенные в программе одной из следующих версий:

- Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента.
- Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Защита без агента.
- Kaspersky Security для виртуальных сред 4.0 Защита без агента.

Сконвертированные политики и задачи имеют название "<название исходной политики или задачи> (конвертированная)".

. Скопировать все сконвертированные политики и задачи из группы администрирования, содержащей кластер KSC для SVM предыдущей версии программы, в группу администрирования, содержащую новый кластер "VMware vCenter Agentless".

Группа администрирования, содержащая кластер KSC для SVM предыдущей версии программы, имеет следующее название: VMware vCenter "<имя сервера VMware vCenter Server, если оно задано>" (<IP-адрес VMware vCenter Server>).

Группа администрирования, содержащая новый кластер "VMware vCenter Agentless", имеет следующее название: VMware vCenter Server '<имя сервера VMware vCenter Server, если оно задано>' (<IP-адрес или доменное имя VMware vCenter Server>) Agentless.

Подробнее о копировании политик и задач см. в документации Kaspersky Security Center.

После завершения обновления программы вы можете удалить политики и задачи, созданные для программы предыдущей версии, а также группу администрирования, содержащую кластер KSC для предыдущей версии программы.

Если вы обновили программу версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента или ниже, вы также можете создавать новые политики на основе имеющихся с помощью мастера создания политики. Для этого на шаге Ввод названия групповой политики требуется установить флажок Использовать параметры политики для предыдущей версии программы (см. подробнее в документации Kaspersky Security Center).

Процедура конвертации политик и задач Kaspersky Security

Чтобы сконвертировать политики и задачи Kaspersky Security предыдущей версии, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. В контекстном меню узла выберите пункт Все задачи → Мастер массовой конвертации политик и задач.

Запустится мастер конвертации политик и задач.

. На первом шаге мастера в списке Название программы выберите Kaspersky Kaspersky Security для виртуальных и облачных сред.

Перейдите к следующему шагу мастера.

. Выберите политики для конвертации. Для этого установите флажок слева от названия политики.

Перейдите к следующему шагу мастера конвертации политик и задач.

Откроется окно Kaspersky Security Network. В этом окне вы можете ознакомиться с Положением о Kaspersky Security Network.

Чтобы продолжить процедуру конвертации политик и задач, внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

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

При необходимости вы сможете изменить это решение позже.

. Выберите задачи для конвертации. Для этого установите флажок слева от названия задачи.

Перейдите к следующему шагу мастера конвертации политик и задач.

. Завершите работу мастера конвертации политик и задач.

Сконвертированные политики получают название "<название исходной политики> (конвертированная)". Сконвертированные задачи получают название "<название исходной задачи> (конвертированная)".

Особенности конвертации политик и задач при обновлении программы

Сконвертированные политики и задачи используют значения параметров политик и задач предыдущей версии программы Kaspersky Security. Параметры, которые отсутствовали в политиках и задачах предыдущей версии программы, принимают значения по умолчанию.

Выбор защищаемой инфраструктуры для политики

Политики конвертируются следующим образом в зависимости от защищаемой инфраструктуры, выбранной в политике предыдущей версии программы:

- Если была выбрана защищаемая инфраструктура и объектам виртуальной инфраструктуры были назначены профили защиты, то в результате конвертации создается политика для одного сервера VMware vCenter Server.

  Защищаемая инфраструктура, выбранная в политике, и назначение профилей защиты объектам виртуальной инфраструктуры сохраняется.

- Если не была выбрана защищаемая инфраструктура, то в результате конвертации создается политика для всей защищаемой инфраструктуры. Всем объектам виртуальной инфраструктуры назначается основной профиль защиты.

Рекомендуется изменить защищаемую инфраструктуру или расположение этой политики в структуре групп администрирования так, чтобы выбранная для политики защищаемая инфраструктура соответствовала расположению политики:

- если политика расположена в группе, которая содержит кластер "VMware vCenter Agentless", в качестве защищаемой инфраструктуры для политики должен быть выбран сервер VMware vCenter Server, соответствующий этому кластеру;
- если политика расположена в папке Управляемые устройства или в группе, которая содержит кластер "VMware vCloud Director Agentless", в качестве защищаемой инфраструктуры для политики должна быть выбрана вся защищаемая инфраструктура.

Вариант действия Выбирать действие автоматически

В сконвертированных политиках и задачах отсутствует вариант действия Выбирать действие автоматически. Если в политике или задаче предыдущей версии программы был выбран этот вариант, в сконвертированной политике или задаче выбирается следующее действие:

- действие при обнаружении угрозы во время защиты виртуальных машин (политика): Лечить. Удалять, если лечение невозможно;
- действие при обнаружении угрозы во время проверки виртуальных машин (задача): для включенных виртуальных машин: Лечить. Удалять, если лечение невозможно; для выключенных виртуальных машин и шаблонов виртуальных машин: Блокировать;
- действие при обнаружении сетевой атаки (политика): Прерывать соединение и блокировать трафик с IP-адреса отправителя;
- действие при обнаружении подозрительной сетевой активности (политика): Прерывать соединение;
- действие при обнаружении принадлежности веб-адреса к категории опасных или нежелательных (политика): Блокировать.

Проверка веб-адресов

Если в политике предыдущей версии программы была включена проверка веб-адресов, в сконвертированной политике параметры проверки веб-адресов принимают следующие значения:

- проверка по базе вредоносных веб-адресов – включена;
- проверка по базе фишинговых веб-адресов – включена, если была включена в политике предыдущей версии программы;
- проверка на принадлежность к категории веб-адресов, которые используются для показа рекламы или связаны с распространением рекламных программ – включена, если в политике предыдущей версии программы была включена проверка по базе вредоносных веб-адресов;
- проверка на принадлежность к категории веб-адресов, связанных с распространением легальных программ, которые могут быть использованы для нанесения вреда виртуальной машине или данным пользователя – выключена.

Если в политике предыдущей версии программы проверка веб-адресов была выключена, в сконвертированной политике она также выключена.

Регистр символов в расширениях файлов

В сконвертированных политиках отсутствует параметр Учитывать регистр символов в сетевых путях. Во время защиты виртуальных машин с операционными системами Windows программа Kaspersky Security не учитывает регистр символов в расширениях файлов, которые требуется исключить из области защиты.

Основной профиль защиты

Профиль защиты, который формируется автоматически при создании политики, в сконвертированных политиках называется "основной профиль защиты". В политиках версии Kaspersky Security для виртуальных сред 4.0 Service Pack 1 Maintenance Release 1 Защита без агента и ниже он назывался "корневой профиль защиты".

Особенности конвертации задач

В сконвертированных задачах выборочной проверки используется область действия задачи, указанная в задачах предыдущей версии программы.

В сконвертированных задачах используется расписание запуска, указанное в задачах предыдущей версии программы.

Изменение параметров Kaspersky Security

С помощью процедуры изменения параметров Kaspersky Security вы можете выполнить следующие действия:

- Изменить параметры подключения Сервера интеграции к VMware NSX Manager, в котором Сервер интеграции регистрирует службы Kaspersky Security.
- Изменить адрес и порт, которые использует VMware NSX Manager для передачи информации на Сервер интеграции.
- Изменить образы SVM, указанные при регистрации служб Kaspersky Security. Если вы изменили адрес расположения образа SVM или выбрали другую конфигурацию SVM, Сервер интеграции повторно зарегистрирует службу с новыми параметрами. После завершения работы мастера изменения параметров вы можете выполнить обновление развернутой службы в консоли VMware vSphere Web Client (раздел Networking & Security → Installation and Upgrade закладка Service Deployments, действие Upgrade). В результате в виртуальной инфраструктуре будут развернуты новые SVM.
- Если при выполнении процедуры регистрации служб Kaspersky Security вы зарегистрировали только одну из двух служб, указать образ SVM для регистрации службы Kaspersky Security, которая не была зарегистрирована. После завершения работы мастера изменения параметров вы можете выполнить процедуру развертывания службы Kaspersky Security на кластерах VMware, чтобы развернуть SVM.
- Изменить следующие параметры конфигурации SVM:
  - IP-адрес Сервера администрирования Kaspersky Security Center и SSL-порт, которые SVM будет использовать для подключения к Kaspersky Security Center.

- Адрес и порт для подключения SVM к Серверу интеграции.
- Пароль конфигурирования и пароль учетной записи root на SVM.
- Часовой пояс, который используется на всех SVM.
- Параметры подключения SVM к сетевому хранилищу данных.

Перечисленные параметры применяются для настройки конфигурации новых SVM, которые вы развернете после завершения работы мастера, а также для изменения конфигурации ранее развернутых SVM с установленными компонентами Kaspersky Kaspersky Security для виртуальных и облачных сред.

Если язык локализации ранее развернутых SVM отличается от языка локализации Консоли Сервера интеграции, в которой вы запускаете процедуру изменения параметров Kaspersky Security, то в результате выполнения процедуры изменяется язык локализации SVM. На SVM применяется язык локализации Консоли Сервера интеграции.

Если вы хотите изменить конфигурацию SVM с установленными компонентами предыдущей версии программы Kaspersky Security, вам требуется отдельно установленная Консоль администрирования Kaspersky Security Center и плагин управления предыдущей версии программы. О процедуре изменения конфигурации SVM предыдущей версии программы см. в документации предыдущей версии программы Kaspersky Security.

Чтобы изменить параметры Kaspersky Security, выполните следующие действия:

. Запустите Консоль Сервера интеграции.

Откроется раздел Защита виртуальной инфраструктуры.

. В списке выберите сервер VMware vCenter Server и разверните список доступных действий щелчком левой клавиши мыши по адресу или имени VMware vCenter Server в графе Адрес.

. В блоке Управление защитой выберите действие Изменить параметры Kaspersky Security.

Запустится мастер изменения параметров. Следуйте указаниям мастера.

Изменение параметров подключений для взаимодействия Сервера интеграции и VMware NSX Manager

На этом шаге вы можете изменить следующие параметры:

- параметры подключения Сервера интеграции к VMware NSX Manager, в котором Сервер интеграции регистрирует службы Kaspersky Security;
- адрес и порт, которые использует VMware NSX Manager для передачи информации на Сервер интеграции.

Если вы хотите изменить параметры подключения Сервера интеграции к VMware NSX Manager, выполните следующие действия:

. Установите флажок Изменить параметры подключения к VMware NSX Manager.

. Укажите следующие параметры подключения:

- 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.

Если вы хотите изменить адрес и порт для подключения VMware NSX Manager к Серверу интеграции, выполните следующие действия:

. Установите флажок Изменить параметры подключения VMware NSX Manager к Серверу интеграции.

. Укажите новые IP-адрес или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции, и порт для подключения.

Перейдите к следующему шагу мастера.

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

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

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

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

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

Изменение образа SVM для службы защиты файловой системы

На этом шаге вы можете выбрать образ SVM с компонентом Защита от файловых угроз. Если выбранный образ SVM отличается от указанного при регистрации службы защиты файловой системы (Kaspersky File Antimalware Protection), Сервер интеграции повторно зарегистрирует службу защиты файловой системы в VMware NSX Manager. После завершения работы мастера изменения параметров вы можете выполнить обновление развернутой службы защиты файловой системы на кластерах VMware. В результате на гипервизорах будут развернуты SVM из нового образа.

Если служба защиты файловой системы ранее не была зарегистрирована, Сервер интеграции зарегистрирует службу защиты файловой системы в VMware NSX Manager. После завершения работы мастера изменения параметров вы можете выполнить развертывание службы защиты файловой системы на кластерах VMware. В результате на гипервизорах будут развернуты SVM с компонентом Защита от файловых угроз.

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

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

Чтобы указать или изменить адрес, по которому расположен образ SVM, выполните следующие действия:

. Установите флажок Указать или изменить образ SVM для службы защиты файловой системы.

. Укажите в поле адрес файла описания образов SVM (файла в формате XML) или адрес OVF-файла образа SVM, соответствующего нужной конфигурации SVM.

. Нажмите на кнопку Проверить.

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

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

- Конфигурация SVM – количество выделенных для SVM процессоров и оперативной памяти.
  Если вы указали адрес файла описания образов SVM (файла в формате XML), вы можете выбрать нужную конфигурацию SVM в раскрывающемся списке в поле Конфигурация SVM.
- Название программы – название программы, которая установлена на SVM.
- Версия SVM – номер версии SVM.
- Производитель – производитель программы, которая установлена на SVM.
- Описание – краткое описание программы.
- Необходимое место на диске – объем дискового пространства, которое требуется для развертывания SVM в хранилище данных.

Перейдите к следующему шагу мастера.

Изменение образа SVM для службы сетевой защиты

На этом шаге вы можете выбрать образ SVM с компонентом Защита от сетевых угроз. Если выбранный образ SVM отличается от указанного при регистрации службы сетевой защиты (Kaspersky Network Protection), Сервер интеграции повторно зарегистрирует службу сетевой защиты в VMware NSX Manager. После завершения работы мастера изменения параметров вы можете выполнить обновление развернутой службы сетевой защиты на кластерах VMware. В результате на гипервизорах будут развернуты SVM из нового образа.

Если служба сетевой защиты ранее не была зарегистрирована, Сервер интеграции зарегистрирует службу сетевой защиты в VMware NSX Manager. После завершения работы мастера изменения параметров вы можете выполнить развертывание службы сетевой защиты на кластерах VMware. В результате на гипервизорах будут развернуты SVM с компонентом Защита от сетевых угроз.

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

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

Чтобы указать или изменить адрес, по которому расположен образ SVM, выполните следующие действия:

. Установите флажок Указать или изменить образ SVM для службы сетевой защиты.

. Укажите в поле адрес файла описания образов SVM (файла в формате XML) или адрес OVF-файла образа SVM, соответствующего нужной конфигурации SVM.

. Нажмите на кнопку Проверить.

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

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

- Конфигурация SVM – количество выделенных для SVM процессоров и оперативной памяти.
  Если вы указали адрес файла описания образов SVM (файла в формате XML), вы можете выбрать нужную конфигурацию SVM в раскрывающемся списке в поле Конфигурация SVM.

- Название программы – название программы, которая установлена на SVM.
- Версия SVM – номер версии SVM.
- Производитель – производитель программы, которая установлена на SVM.
- Описание – краткое описание программы.
- Необходимое место на диске – объем дискового пространства, которое требуется для развертывания SVM в хранилище данных.

Перейдите к следующему шагу мастера.

Просмотр сведений о режиме обработки трафика для компонента Защита от сетевых угроз

На этом шаге отображается информация о режиме обработки трафика, выбранном при регистрации службы сетевой защиты:

- Стандартный режим. Если выбран этот режим, виртуальный фильтр (VMware DVFilter) перехватывает трафик виртуальных машин и передает на проверку программе Kaspersky Security. При обнаружении признаков вторжений или попытки доступа к опасным или нежелательным веб-адресам Kaspersky Security выполняет то действие, которое указано в параметрах политики, и передает информацию о событиях на Сервер администрирования Kaspersky Security Center.
- Режим мониторинга. Если выбран этот режим, программа Kaspersky Security получает копию трафика виртуальных машин. При обнаружении признаков вторжений или попытки доступа к опасным или нежелательным веб-адресам Kaspersky Security не предпринимает действий по предотвращению угроз, а только передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

Для компонента Защита от сетевых угроз, установленного на уже развернутых SVM, невозможно изменить режим обработки трафика. Чтобы выбрать другой режим обработки трафика, вам потребуется удалить SVM, отменить регистрацию службы сетевой защиты, а затем повторно выполнить регистрацию службы сетевой защиты с новым режимом обработки трафика и развернуть новые SVM.

Перейдите к следующему шагу мастера.

Изменение параметров подключений для SVM

На этом шаге вы можете изменить следующие параметры подключений для SVM:

- IP-адрес Сервера администрирования Kaspersky Security Center и SSL-порт, которые SVM будет использовать для подключения к Kaspersky Security Center;
- адрес и порт для подключения SVM к Серверу интеграции.

Если вы хотите изменить IP-адрес и порт для подключения SVM к Серверу администрирования Kaspersky Security Center, выполните следующие действия:

. Установите флажок Изменить параметры подключения SVM к Kaspersky Security Center.

. Укажите новые IP-адрес Сервера администрирования Kaspersky Security Center и SSL-порт, которые SVM будет использовать для подключения к Kaspersky Security Center.

Если вы хотите изменить адрес и порт для подключения SVM к Серверу интеграции, выполните следующие действия:

. Установите флажок Изменить параметры подключения SVM к Серверу интеграции.

. Укажите новые IP-адрес или полное доменное имя (FQDN) компьютера, на котором установлен Сервер интеграции, и порт для подключения.

Перейдите к следующему шагу мастера.

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

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

Изменение паролей учетных записей на SVM

На этом шаге вы можете изменить пароль учетной записи klconfig (пароль конфигурирования) и пароль учетной записи root. Указанные пароли будут использоваться на всех SVM, которые вы развернете после повторной регистрации служб Kaspersky Security, а также на ранее развернутых SVM. Пароль конфигурирования требуется для изменения конфигурации SVM. Учетная запись root используется для доступа к операционной системе на SVM и к файлам трассировки SVM.

Если вы хотите изменить пароль конфигурирования, выполните следующие действия:

. Установите флажок Изменить пароль учетной записи klconfig (пароль конфигурирования).

. Введите новый пароль в полях Пароль и Подтверждение пароля.

Если вы хотите изменить пароль учетной записи root, выполните следующие действия:

. Установите флажок Изменить пароль учетной записи root.

. Введите новый пароль в полях Пароль и Подтверждение пароля.

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

Перейдите к следующему шагу мастера.

Изменение часового пояса для SVM

На этом шаге вы можете изменить часовой пояс, который используется на SVM. Указанный часовой пояс будет использоваться на всех SVM, которые вы развернете после повторной регистрации служб Kaspersky Security, а также на ранее развернутых SVM.

Чтобы изменить часовой пояс на SVM, установите флажок Изменить часовой пояс для SVM и выберите значение в раскрывающемся списке.

Перейдите к следующему шагу мастера.

Изменение параметров подключения к сетевому хранилищу данных

На этом шаге вы можете настроить следующие параметры использования сетевого хранилища данных: разрешить

- или запретить использование сетевого хранилища данных для SVM; указать или изменить ранее указанные
- параметры подключения SVM к сетевому хранилищу данных.

Сетевое хранилище данных может использоваться для хранения резервных копий файлов, помещенных в резервные хранилища на SVM.

Если вы хотите настроить параметры использования сетевого хранилища данных, выполните следующие действия:

. Установите флажок Изменить параметры подключения к сетевому хранилищу данных.

. Если SVM не должны использовать сетевое хранилище данных, выберите вариант Не использовать сетевое хранилище данных.

. Если вы хотите разрешить использование сетевого хранилища данных для SVM, выберите вариант Использовать сетевое хранилище данных и укажите следующие параметры подключения к хранилищу:

- Адрес сетевого хранилища данных в формате UNC.

  В качестве адреса не может быть указано localhost или 127.0.0.1.

- Учетную запись, с которой SVM должны подключаться к сетевому хранилищу данных, в виде <домен>\<имя пользователя>.
- Пароль учетной записи для подключения.

Перейдите к следующему шагу мастера.

Мастер проверит возможность подключения к сетевому хранилищу данных с указанными параметрами.

Если проверка параметров подключения завершилась с ошибкой, в окне мастера отображается сообщение об ошибке, переход к следующему шагу мастера невозможен. Если вы хотите исправить введенные параметры, нажмите на кнопку Отмена. Если

параметры введены правильно, вы можете игнорировать сообщение об ошибке. В этом случае нажмите на кнопку Продолжить, чтобы перейти к следующему шагу мастера.

Запуск изменения параметров Kaspersky Security

На этом шаге вы можете посмотреть информацию о параметрах, которые будут изменены в результате выполнения процедуры.

> В списке изменяемых параметров указывается язык локализации SVM, если язык локализации Консоли Сервера интеграции, в которой вы запускаете процедуру изменения параметров Kaspersky Security, отличается от языка локализации ранее развернутых SVM. На всех SVM будет использоваться язык локализации Консоли Сервера интеграции.

Перейдите к следующему шагу мастера, чтобы запустить изменение параметров.

Процесс изменения параметров Kaspersky Security

На этом шаге отображается информация о действиях, которые выполняет Сервер интеграции, чтобы применить новые параметры.

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

После выполнения всех действий перейдите к следующему шагу мастера.

Завершение работы мастера

На этом шаге отображается информация о результатах изменения параметров Kaspersky Security.

Если изменение параметров завершилось успешно, завершите работу мастера.

Если изменение параметров завершилось 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 файлах трассировки Сервера интеграции (если вы включили запись информации в файлы трассировки Сервера интеграции).

Удаление программы

Вы можете удалить программу Kaspersky Security полностью или удалить только один из компонентов программы (Защита от файловых угроз или Защита от сетевых угроз).

Если вы хотите удалить программу Kaspersky Security полностью, вам требуется выполнить следующие действия:

. Удалить в виртуальной инфраструктуре VMware оба компонента Kaspersky Security (Защита от файловых угроз и Защита от сетевых угроз).

. Отменить регистрацию в VMware NSX Manager обеих служб Kaspersky Security.

Отмена регистрации служб Kaspersky Security выполняется в Консоли Сервера интеграции. Также будет отменена регистрация Сервера интеграции (Kaspersky Service Manager) в VMware NSX Manager.

. Удалить плагин управления Kaspersky Security и Сервер интеграции.

. Если вы использовали программу в режиме multitenancy, вам нужно также удалить плагин управления Kaspersky Security для клиентов и виртуальные Серверы администрирования Kaspersky Security Center, которые были созданы для управления защитой виртуальных машин клиентов.

Подробнее об удалении виртуальных Серверов администрирования см. в документации Kaspersky Security Center.

Если вы хотите удалить один из компонентов программы Kaspersky Security, вам требуется выполнить следующие действия:

. Удалить в виртуальной инфраструктуре VMware компонент Kaspersky Security (Защита от файловых угроз или Защита от сетевых угроз).

. Отменить регистрацию в VMware NSX Manager службы Kaspersky Security, соответствующей удаленному компоненту (Kaspersky File Antimalware Protection или Kaspersky Network Protection).

При удалении SVM с компонентом Защита от файловых угроз автоматически удаляются копии файлов, помещенные в резервное хранилище на SVM. Если для SVM было включено использование сетевого хранилища данных, резервные копии файлов с этой SVM сохраняются в отдельной папке в сетевом хранилище данных.

После удаления компонентов Защита от файловых угроз и Защита от сетевых угроз SVM продолжают отображаться в Консоли администрирования Kaspersky Security Center. По истечении срока, установленного в параметрах Kaspersky Security Center (см. в документации Kaspersky Security Center), SVM автоматически удаляются из Консоли администрирования. Вы можете вручную удалить SVM из Консоли администрирования Kaspersky Security Center сразу после завершения процедуры удаления программы.

До удаления SVM из Консоли администрирования Kaspersky Security Center события, отправленные этими SVM, сохраняются в Kaspersky Security Center и отображаются в отчетах и журнале событий Kaspersky Security Center.

Список резервных копий файлов, помещенных в резервное хранилище на SVM с компонентом Защита от файловых угроз, также сохраняется в Kaspersky Security Center, но действия с резервными копиями файлов недоступны.

Удаление компонентов Kaspersky Security в виртуальной инфраструктуре VMware

Для удаления компонента Защита от файловых угроз в виртуальной инфраструктуре VMware требуется выполнить следующие действия:

. Удалить все SVM с компонентом Защита от файловых угроз на кластерах VMware.

Удаление SVM выполняется путем удаления развернутой на кластерах VMware службы защиты файловой системы (Kaspersky File Antimalware Protection).

Удаление выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Installation and Upgrade на закладке Service Deployments). В списке развернутых сетевых служб и служб обеспечения защиты виртуальных машин требуется удалить службу Kaspersky File Antimalware Protection, развернутую на кластерах, на которых вы хотите удалить SVM (см. подробнее в Базе знаний).

. Удалить политику безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).

Удаление политики безопасности NSX выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Service Composer на закладке Security Policies). Для выбранной политики необходимо выполнить действие Actions → Delete.

Вы можете также удалить группу безопасности NSX (NSX Security Group), в которую включены защищаемые виртуальные машины.

Удаление группы безопасности NSX выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Service Composer на закладке Security Groups).

Подробнее об удалении политики безопасности NSX и группы безопасности NSX см. в Базе знаний .

Для удаления компонента Защита от сетевых угроз в виртуальной инфраструктуре VMware требуется выполнить следующие действия:

. Удалить все SVM с компонентом Защита от сетевых угроз на кластерах VMware.
Удаление SVM выполняется путем удаления развернутой на кластерах VMware службы сетевой защиты (Kaspersky Network Protection).

Удаление выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Installation and Upgrade на закладке Service Deployments). В списке развернутых сетевых служб и служб обеспечения защиты виртуальных машин требуется удалить службу Kaspersky Network Protection, развернутую на кластерах, на которых вы хотите удалить SVM (см. подробнее в Базе знаний).

. Удалить политику безопасности NSX (NSX Security Policy), в которой настроено использование службы сетевой защиты (Kaspersky Network Protection).

Удаление политики безопасности NSX выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Service Composer на закладке Security Policies). Для выбранной политики необходимо выполнить действие Actions → Delete.

Вы можете также удалить группу безопасности NSX (NSX Security Group), в которую включены защищаемые виртуальные машины.

Удаление группы безопасности NSX выполняется в консоли VMware vSphere Web Client (в разделе Networking & Security → Service Composer на закладке Security Groups).

Подробнее об удалении политики безопасности NSX и группы безопасности NSX см. в Базе знаний .

Отмена регистрации служб Kaspersky Security и Сервера интеграции

Отмена регистрации службы Kaspersky Security возможна, только если на кластерах VMware удалены все SVM и служба не используется в политиках безопасности NSX (NSX Security Policy).

Чтобы отменить регистрацию служб Kaspersky Security в VMware NSX Manager, выполните следующие действия:

. Запустите Консоль Сервера интеграции.

Откроется раздел Защита виртуальной инфраструктуры.

. В списке выберите сервер VMware vCenter Server и разверните список доступных действий щелчком левой клавиши мыши по адресу или имени VMware vCenter Server в графе Адрес.

. В блоке Управление защитой выберите действие Отменить регистрацию служб Kaspersky Security.

. В открывшемся окне выполните одно из следующих действий:

- Если вы удаляете компонент Защита от файловых угроз, установите флажок Служба защиты файловой системы (Kaspersky File Antimalware Protection).
- Если вы удаляете компонент Защита от сетевых угроз, установите флажок Служба сетевой защиты (Kaspersky Network Protection).
- Если вы удаляете программу полностью, установите оба флажка. В VMware NSX Manager будет отменена регистрация обеих служб Kaspersky Security, а также регистрация Сервера интеграции (Kaspersky Service Manager).

Если регистрация одной из служб Kaspersky Security уже отменена, флажок недоступен.

. Нажмите на кнопку ОК.

Если отмена регистрации служб Kaspersky Security и Сервера интеграции завершается с ошибкой, вы можете отменить регистрацию служб и Сервера интеграции вручную в консоли VMware vSphere Web Client (см. подробнее в Базе знаний).

Удаление основного плагина управления Kaspersky Security и Сервера интеграции

Вы можете удалить основной плагин управления Kaspersky Security, Сервер интеграции и Консоль Сервера интеграции одним из следующих способов:

- В интерактивном режиме с использованием стандартных средств удаления программ в операционной системе. В списке программ требуется выбрать для удаления Kaspersky Kaspersky Security для виртуальных и облачных сред – компоненты управления. Удаление выполняется с помощью мастера.
- В тихом режиме из командной строки. В командной строке требуется ввести следующую команду:

  `ksv-components_6.0.0.XXX_mlg.exe –q –uninstall`

  где `6.0.0.XXX` – номер версии программы.

При удалении Сервера интеграции с помощью мастера вы можете сохранить следующие данные, используемые в работе Сервера интеграции:

- SSL-сертификат, который используется для установки защищенного соединения с Сервером интеграции; данные,
- сохраненные Сервером интеграции во время работы; файлы трассировки Сервера интеграции и Консоли Сервера
- интеграции.

Если вы хотите сохранить указанные данные, в окне запроса о сохранении данных нажмите на кнопку Сохранить. Сохраненные данные и параметры автоматически используются при повторной установке Сервера интеграции.

Удаление плагина управления Kaspersky Security для клиентов

Вы можете удалить плагин управления Kaspersky Security для клиентов одним из следующих способов:

- В интерактивном режиме с использованием стандартных средств удаления программ в операционной системе.

  В списке программ требуется выбрать для удаления Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) – плагин управления. Удаление выполняется с помощью мастера.

- В тихом режиме из командной строки. В командной строке требуется ввести следующую команду:

  `ksv-t-components_6.0.0.XXX_mlg.exe –q –uninstall`

  где `6.0.0.XXX` – номер версии программы.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки плагина управления Kaspersky Security и Сервера интеграции.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

После установки программы вы можете ознакомиться с текстом Лицензионного соглашения и с Политикой конфиденциальности, которая описывает обработку и передачу данных, следующими способами:

- В файле на компьютере, где установлен плагин управления Kaspersky Security, Сервер интеграции и / или Консоль Сервера интеграции:

%ProgramFiles(x86)%\Kaspersky Lab\KSV\Kaspersky Security for Virtualization 6.0 Agentless\EULA\license_<идентификатор языка>.txt, где <идентификатор языка> – идентификатор языка локализации установленных компонентов Kaspersky Security.

- В окне настройки параметров развернутой SVM на закладке vApp в консоли VMware vSphere Web Client или VMware vSphere Client.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О предоставлении данных

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- При обновлении баз Kaspersky Security: идентификатор
  - Kaspersky Security; идентификатор действующей лицензии;
  - уникальный идентификатор установки Kaspersky Security;
  - уникальный идентификатор запуска задачи обновления;
  - полную версию Kaspersky Security.
- При переходе по ссылкам из интерфейса Kaspersky Security:
  - тип программы Kaspersky Security;
  - версию Kaspersky Security; язык
  - интерфейса Kaspersky Security;

  идентификатор веб-страницы, на

  которую выполняется переход.

- Если для активации Kaspersky Security применяется код активации:
  - идентификатор, версию и локализацию программы Kaspersky Security, а также идентификаторы

    совместимых программ; идентификатор SVM и уникальный идентификатор установки Kaspersky Security;
  - код активации и время активации программы;
  -
  -

тип, версию и разрядность операционной системы, название виртуальной среды, в которой установлена программа Kaspersky Security;
- информацию об упаковке регулярно передаваемых подтверждений статуса лицензионного ключа.

Информация передается периодически с целью проверки правомерности использования программы.

Кроме того, вы соглашаетесь передавать следующую информацию:

- тип, версию и локализацию программы Kaspersky Security;
- тип и версию гипервизора, на котором развернута SVM, а также тип, версию и разрядность операционной системы на защищенной виртуальной машине и примерное количество виртуальных машин, на которых установлена эта операционная система; универсальный уникальный идентификатор SVM; вид лицензии, номер заказа лицензии, тип
- используемой схемы лицензирования;
- количество единиц лицензирования, для которых ключ может использоваться, и количество единиц лицензирования,
- для которых ключ уже используется.

"Лаборатория Касперского" может использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Используя код активации, вы соглашаетесь на автоматическую передачу в "Лабораторию Касперского" данных, перечисленных выше. Если вы не согласны предоставлять эту информацию, для активации Kaspersky Security следует использовать файл ключа.

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.

Более подробную информацию об обработке, хранении и уничтожении информации, полученной во время использования программы и переданной в "Лабораторию Касперского", вы можете получить, ознакомившись с Политикой конфиденциальности на веб-сайте "Лаборатории Касперского".

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих услуг:

- Использование программы в соответствии с условиями Лицензионного соглашения для защиты виртуальных машин на гипервизорах VMware ESXi.
- Получение технической поддержки.

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

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию. Вы можете активировать программу по пробной лицензии только один раз.

- Коммерческая – платная лицензия, которая предоставляется при приобретении программы.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Вы по-прежнему можете защищать виртуальные машины и выполнять их проверку, но только на основе баз программы, установленных до истечения срока действия лицензии. Чтобы продолжить использование Kaspersky Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии. Рекомендуется продлевать срок действия коммерческой лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

Функциональность программы, доступная по коммерческой лицензии, зависит от вида лицензии. Для программы Kaspersky Security предусмотрены следующие виды лицензии:

- стандартная лицензия; расширенная
- лицензия.

Функция обнаружения подозрительной сетевой активности доступна, только если вы используете программу по расширенной лицензии.

Для Kaspersky Security предусмотрены следующие схемы лицензирования:

- Лицензирование по количеству виртуальных машин, защищаемых с помощью программы. Для этой схемы лицензирования используются ключи для серверов и ключи для рабочих станций (в зависимости от типа операционной системы защищаемых виртуальных машин). В соответствии с лицензионным ограничением программа используется для защиты определенного количества виртуальных машин.
- Лицензирование по количеству ядер, используемых в физических процессорах на всех гипервизорах, на которых установлены SVM. Для этой схемы лицензирования используются ключи с ограничением по ядрам. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, развернутых на гипервизорах, в которых используется определенное количество ядер физических процессоров.
- Лицензирование по количеству процессоров, используемых на гипервизорах, на которых работают защищенные виртуальные машины. Для этой схемы лицензирования используются ключи с ограничением по процессорам. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, развернутых на гипервизорах, в которых используется определенное количество процессоров.

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

Если вы используете схему лицензирования по количеству виртуальных машин, защищаемых с помощью программы, при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены.

Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин одним из следующих способов:

- Выключить защиту виртуальной машины.
- Исключить виртуальную машину из группы безопасности NSX (NSX Security Group) с назначенной политикой безопасности NSX (NSX Security Policy), в которой настроено использование службы защиты файловой системы (Kaspersky File Antimalware Protection).
- Перенести виртуальную машину на гипервизор, на котором не развернута SVM.

В рамках одного сервера VMware vCenter Server вы можете использовать только одну из предусмотренных схем лицензирования.

О Лицензионном сертификате

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

> Если вы используете программу по подписке, Лицензионный сертификат не предоставляется.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- информация о пользователе, которому предоставляется лицензия; информация о программе, которую
- можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать

программу по предоставляемой лицензии); дата начала срока действия лицензии; дата окончания срока действия

- лицензии или срок действия лицензии; тип лицензии.
-

О лицензионном ключе

Лицензионный ключ (далее также "ключ") – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу одним из следующих способов:

- применить файл ключа; ввести
- код активации.

Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

После добавления ключей вы можете заменять их другими.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, вы можете обратиться к продавцу лицензии или добавить другой ключ для работы программы.

Для Kaspersky Security используются лицензионные ключи следующих типов:

- Ключ для серверов – ключ программы для защиты виртуальных машин с операционными системами для серверов.
- Ключ для рабочих станций – ключ программы для защиты виртуальных машин с операционными системами для рабочих станций.
- Ключ с ограничением по ядрам – ключ программы для защиты виртуальных машин независимо от установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты виртуальных машин, работающих на гипервизорах, в которых используется определенное количество ядер физических процессоров.
- Ключ с ограничением по процессорам – ключ программы для защиты виртуальных машин независимо от установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, работающих на гипервизорах, в которых используется определенное количество процессоров.

Лицензионный ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для пробной лицензии, ключ для коммерческой лицензии (коммерческий ключ) или ключ по подписке. На одну SVM не может быть добавлено больше одного активного ключа каждого типа (ключ для серверов, ключ для рабочих станций, ключ с ограничением по ядрам, ключ с ограничением по процессорам). Если SVM используется в виртуальной инфраструктуре для защиты виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций, на нее добавляется два ключа: ключ для серверов и ключ для рабочих станций.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом.

Дополнительный ключ может быть добавлен только при наличии активного ключа того же типа. Активный и дополнительный ключи должны соответствовать одному типу лицензии.

Ключ для пробной лицензии и ключ по подписке могут быть добавлены только в качестве активного ключа.
Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве дополнительного ключа. Ключ для пробной лицензии не может заменить активный коммерческий ключ.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

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

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

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно обратиться к продавцу лицензии.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security или после заказа пробной версии Kaspersky Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации вам нужно обратиться к продавцу лицензии.

О подписке

Подписка на Kaspersky Security – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security можно оформить у поставщика услуг (например, у интернет-провайдера).

Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отказаться от нее. Для управления подпиской вам нужно связаться с поставщиком услуг, у которого вы приобрели Kaspersky Security.

> В зависимости от поставщика услуг, набор возможных действий при управлении подпиской может различаться.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security после окончания ограниченной подписки вам нужно продлить ее. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка приостановлена, вам может предоставляться льготный период для продления подписки, в течение которого программа продолжает выполнять все свои функции. Наличие и длительность льготного периода определяет поставщик услуг.

По истечении подписки или льготного периода для продления подписки, если он предоставлен, Kaspersky Security продолжает работу, но прекращает обновлять базы программы и использовать Kaspersky Security Network.

В зависимости от поставщика услуг, по истечении подписки и льготного периода функциональность программы может ограничиваться следующим образом: Kaspersky Security прекращает обновлять базы программы, использовать Kaspersky Security Network, а также прекращает защищать виртуальные машины и выполнять их проверку. Для получения подробной информации об ограничении функциональности программы по истечении подписки и льготного периода обращайтесь к поставщику услуг, у которого вы приобрели Kaspersky Security.

Чтобы использовать Kaspersky Security по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации в программу добавляется ключ по подписке – активный ключ, соответствующий лицензии на использование программы по подписке.

Ключ по подписке может быть добавлен только в качестве активного ключа. Нельзя добавить ключ по подписке в качестве дополнительного ключа.

Об активации программы

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

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

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

Вы можете добавить ключ в хранилище ключей Kaspersky Security Center одним из следующих способов:

- с помощью файла ключа; с
- помощью кода активации.

Вы можете добавить ключ в хранилище ключей Kaspersky Security Center во время создания задачи активации программы на SVM или предварительно.

Условия активации программы с помощью кода активации

Для добавления ключа с помощью кода активации необходимо подключение к серверам активации "Лаборатории Касперского". Мастер добавления ключа в хранилище отправляет данные на серверы активации "Лаборатории Касперского", чтобы проверить введенный код активации. Подключение к серверам активации обеспечивает служба прокси-сервера активации. Если служба прокси-сервера активации выключена, добавление ключа в хранилище с помощью кода активации невозможно. Если доступ в интернет осуществляется через прокси-сервер, в свойствах Сервера администрирования Kaspersky Security Center должны быть настроены параметры прокси-сервера.

Подробнее о службе прокси-сервера активации см. в документации Kaspersky Security Center.

Особенности добавления ключей разных типов

При добавлении ключей следует учитывать следующие особенности:

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

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

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

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

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

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

- Не поддерживается одновременное использование на SVM коммерческих ключей и ключей по подписке.

  Например, если вы добавляете коммерческий ключ, а ранее на SVM был добавлен ключ по подписке, то ключ по подписке удаляется с SVM. Вместо него добавляется коммерческий ключ.

- Не поддерживается одновременное использование на SVM ключей, которые соответствуют разным видам лицензии (стандартная лицензия или расширенная лицензия).

  Например, если вы добавляете ключ, соответствующий расширенной лицензии, а ранее программа использовалась по стандартной лицензии, то все активные и (при наличии) дополнительные ключи, соответствующие стандартной лицензии, удаляются с SVM. Вместо них добавляется ключ, соответствующий расширенной лицензии.

Процедура активации программы

Чтобы активировать программу, выполните следующие действия:

. Создайте задачу активации программы. Вы можете создать задачу активации программы для всех SVM, для SVM одного кластера KSC или для отдельной SVM.

При создании задачи активации программы используется ключ из хранилища ключей Kaspersky Security Center. Вы можете добавить ключ в хранилище ключей Kaspersky Security Center предварительно или во время создания задачи активации программы.

> Если программа используется по подписке, в течение льготного периода невозможно создать задачу активации. Вы можете использовать ранее созданную задачу активации программы для добавления ключа.

. Запустите задачу активации программы.

Задача активирует программу на тех SVM, где отсутствовал активный ключ, и заменит старый ключ на новый на тех SVM, где программа уже активирована.

Если на вашу SVM добавлены и ключ для серверов, и ключ для рабочих станций, то сроком использования программы является наиболее длительный из двух сроков: срок использования программы с ключом для серверов или срок использования программы с ключом для рабочих станций.

Если количество единиц лицензирования, для которых используется ключ, превышает количество, указанное в Лицензионном сертификате, Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center событие с информацией о нарушении лицензионных ограничений (см. в документации Kaspersky Security Center).

Добавление ключа в хранилище ключей Kaspersky Security Center

Чтобы добавить ключ в хранилище ключей Kaspersky Security Center, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center запустите мастер добавления ключа в хранилище:

a. В дереве консоли выберите папку Лицензии Лаборатории Касперского.

b. В рабочей области нажмите на кнопку Добавить код активации или ключ.

. В окне мастера Выбор способа активации программы выберите способ добавления ключа в хранилище:

- Нажмите на кнопку Активировать программу с помощью кода активации, если вы хотите добавить ключ с помощью кода активации.

- Нажмите на кнопку Активировать программу с помощью файла ключа, если вы хотите добавить ключ с помощью файла ключа.

. В зависимости от выбранного вами способа добавления ключа, выполните одно из следующих действий:

- Введите код активации.

- Укажите путь к файлу ключа. Для этого нажмите на кнопку Обзор и в открывшемся окне выберите файл с расширением key.

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

. Завершите работу мастера добавления ключа в хранилище.

Добавленный ключ отобразится в списке ключей в папке Лицензии Лаборатории Касперского дерева консоли.

Ключи, добавленные в хранилище ключей Kaspersky Security Center, вы можете использовать при создании задачи активации программы на SVM.

Создание задачи активации программы

Чтобы создать задачу активации программы, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите нужную папку или группу администрирования:

- Если вы хотите активировать программу на всех SVM, выберите папку Управляемые устройства главного Сервера администрирования Kaspersky Security Center. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

- Если вы хотите активировать программу на SVM одного кластера KSC, в папке Управляемые устройства дерева консоли выберите группу администрирования, содержащую этот кластер KSC. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

- Если вы хотите активировать программу на одной или нескольких SVM, выполните одно из следующих действий:

  - Откройте папку Задачи дерева консоли. Нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

  - В дереве консоли выберите папку Лицензии Лаборатории Касперского. Нажмите на кнопку Распространить ключ на управляемые устройства, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите тип задачи.

- Если вы запустили мастер создания задачи из папки Управляемые устройства или из папки Задачи, выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред → Активация программы.

- Если вы запустили мастер создания задачи из папки Лицензии Лаборатории Касперского, укажите программу, для которой создается задача: Kaspersky Kaspersky Security для виртуальных и облачных сред.

Перейдите к следующему шагу мастера создания задачи.

. Чтобы выбрать ключ из хранилища ключей Kaspersky Security Center, нажмите на кнопку Выбрать. Откроется окно Выбор лицензионного ключа.

Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ и нажмите на кнопку ОК.

Если нужный ключ в хранилище ключей отсутствует, добавьте его следующим образом:

a. Нажмите на кнопку Добавить, расположенную справа в верхней части окна Выбор лицензионного ключа. Запустится мастер добавления ключа в хранилище ключей Kaspersky Security Center.

b. Следуйте указаниям мастера, чтобы добавить ключ в хранилище ключей.

c. Завершите работу мастера добавления ключа в хранилище.

После завершения работы мастера выберите добавленный ключ в окне Выбор лицензионного ключа и нажмите на кнопку ОК.

В нижней части окна отобразится информация о выбранном ключе.

Если вы хотите использовать добавленный ключ как дополнительный, установите флажок Использовать лицензионный ключ в качестве дополнительного.

> Флажок недоступен, если вы добавляете ключ для пробной лицензии или ключ по подписке. Невозможно добавить ключ для пробной лицензии и ключ по подписке в качестве дополнительного ключа.

Перейдите к следующему шагу мастера создания задачи.

. Если вы запустили мастер создания задачи из папки Задачи или из папки Лицензии Лаборатории Касперского, укажите способ выбора SVM, на которых должна выполняться задача:

- Нажмите на кнопку Выбрать устройства, обнаруженные в сети Сервером администрирования, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.

- Нажмите на кнопку Задать адреса устройств вручную или импортировать из списка, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

> Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку Назначить задачу выборке устройств, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.

- Нажмите на кнопку Назначить задачу группе администрирования, если задача должна выполняться на всех SVM, входящих в группу администрирования.

  В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

  - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.
  - Нажмите на кнопку Добавить или Добавить IP-диапазон и задайте адреса SVM.
  - Нажмите на кнопку Импортировать и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
  - Нажмите на кнопку Обзор и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
  - Нажмите на кнопку Обзор и выберите группу администрирования или введите название группы администрирования вручную.

Перейдите к следующему шагу мастера создания задачи.

. Настройте расписание 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.

- Использовать случайную задержку запуска задачи в интервале (мин). Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок Использовать автоматическое определение случайного интервала между запусками задачи.

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

Перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера 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.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу активации программы вручную.

Продление срока действия лицензии

Когда срок действия лицензии подходит к концу, вы можете продлить его, добавив дополнительный ключ. Это позволит избежать ограничения функциональности программы в период после истечения срока действия лицензии и до активации программы по новой лицензии.

Для добавления дополнительного ключа на SVM используется задача активации программы.

Невозможно добавить дополнительный ключ, если вы используете программу по подписке.

Тип дополнительного ключа должен соответствовать типу ранее добавленного активного ключа.

Если вы используете схему лицензирования по количеству защищенных виртуальных машин, тип дополнительного ключа должен соответствовать типу гостевой операционной системы виртуальных машин: для виртуальных машин с операционными системами для серверов предназначен дополнительный ключ для серверов, для виртуальных машин с операционными системами для рабочих станций – дополнительный ключ для рабочих станций.

Если SVM используется в виртуальной инфраструктуре для защиты виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций, на SVM рекомендуется добавить два дополнительных ключа: ключ для серверов и ключ для рабочих станций.

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

Дополнительный ключ должен соответствовать тому же виду лицензии, что и активный ключ (стандартная лицензия или расширенная лицензия).

Чтобы продлить срок действия лицензии, выполните следующие действия:

. Создайте задачу активации программы для SVM, на которые вы хотите добавить дополнительный ключ. Вы можете создать задачу для всех SVM, для SVM одного кластера KSC или для отдельной SVM.

. Установите флажок Использовать лицензионный ключ в качестве дополнительного на втором шаге мастера создания задачи.

. Запустите задачу активации программы.

В результате выполнения задачи дополнительный ключ добавляется на те SVM в составе кластера KSC, на которые уже добавлен активный ключ. Дополнительный ключ автоматически начнет использоваться в качестве активного ключа по истечении срока действия лицензии на использование Kaspersky Security.

Если для активации программы вы применяете код активации, по истечении срока действия лицензии программа автоматически подключается к серверам активации "Лаборатории Касперского" для замены активного ключа с истекшим сроком годности. Если автоматическое подключение программы к серверам активации "Лаборатории Касперского" завершается с ошибкой, требуется вручную запустить задачу активации программы, чтобы продлить срок действия лицензии на использование Kaspersky Security.

Задача активации программы на SVM завершается с ошибкой и дополнительный ключ не добавляется, если выполняется одно из следующих условий:

- активный ключ отсутствует на SVM; в качестве активного ключа добавлен ключ по подписке; тип добавляемого
- дополнительного ключа не соответствует типу ранее добавленного активного ключа.
- Если на SVM добавлены активный и дополнительный ключи и вы заменяете активный ключ, Kaspersky Security проверяет дату окончания срока годности дополнительного ключа. Если срок годности дополнительного ключа истекает ранее продленного срока действия лицензии, Kaspersky Security автоматически удаляет дополнительный ключ. В этом случае после добавления активного ключа вы можете добавить другой дополнительный ключ.

Продление подписки

Во время использования программы по подписке Kaspersky Security обращается к серверам активации "Лаборатории Касперского" через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете программу по неограниченной подписке, Kaspersky Security в фоновом режиме проверяет наличие нового ключа на серверах активации "Лаборатории Касперского" и, в случае его наличия, добавляет новый ключ вместо предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Security продлевается без вашего участия.

Если вы используете программу по ограниченной подписке, в день истечения подписки или льготного периода, в течение которого доступно продление подписки, Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию об этом и прекращает попытки автоматического продления подписки. Kaspersky Security прекращает обновлять базы программы и использовать Kaspersky Security Network.
Вы можете продлить подписку, связавшись с поставщиком услуг, у которого вы приобрели Kaspersky Security.

После продления подписки вам требуется повторно запустить задачу добавления ключа, которую вы создали для добавления ключа по подписке.

Просмотр информации об используемых ключах

Информацию об используемых ключах вы можете просмотреть в Консоли администрирования Kaspersky Security Center:

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

Просмотр информации о ключе в папке Лицензии Лаборатории Касперского

Чтобы просмотреть информацию о ключе в папке Лицензии Лаборатории Касперского, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Лицензии Лаборатории Касперского.

В рабочей области отобразится список ключей, добавленных в хранилище ключей Kaspersky Security Center.

. В списке ключей выберите ключ, информацию о котором вы хотите просмотреть.

Справа от списка ключей отобразится следующая информация о ключе:

- <Уникальная буквенно-цифровая последовательность> (ключ).
- Программа – название программы, для которой предназначен ключ, и информация о лицензии.
- Тип – тип лицензии. Возможные варианты: пробная, коммерческая или подписка.
- Срок действия (сут) – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа (например, 365 дней). Если вы используете программу по подписке, в поле отображается <Недоступно>.
- Дата окончания срока годности – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать программу можно только до истечения этого срока. Если вы используете программу по неограниченной подписке, в поле отображается Неограниченная.

- Дата окончания срока действия лицензии – дата окончания срока использования программы, активированной путем добавления этого ключа. Если вы используете программу по неограниченной подписке, в поле отображается Неограниченная.

- Ограничение – в зависимости от типа ключа:

  - Для ключа для серверов – максимальное количество виртуальных машин с операционной системой для серверов, которые вы можете защищать.

  - Для ключа для рабочих станций – максимальное количество виртуальных машин с операционной системой для рабочих станций, которые вы можете защищать.

    Для ключа для серверов и ключа для рабочих станций при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены. Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин.

  - Для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

  - Для ключа с ограничением по процессорам – максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

- Устройств, на которых ключ является активным – количество SVM, на которые ключ добавлен в качестве активного.

- Устройств, на которых ключ является дополнительным – количество SVM, на которые ключ добавлен в качестве дополнительного.

Если вы выбрали в списке ключ по подписке, то справа от списка ключей также отображается следующая информация:

- Тип ограничения срока действия – если программа используется по неограниченной подписке, в поле отображается Неограниченная. Если подписка ограниченная, то поле не отображается.

- Льготный период – количество дней после приостановки подписки, в течение которых программа продолжает выполнять все свои функции.

- Веб-адрес провайдера подписки – веб-адрес поставщика услуг, у которого зарегистрирована подписка.

- Состояние подписки – текущий статус подписки. Возможные значения: Активна, Приостановлена, Истекла, Отменена, Активирован льготный период.

Сведения о подписке отображаются также в окне свойства ключа по подписке в разделе О подписке.

Если на SVM добавлены и ключ для серверов, и ключ для рабочих станций, в папке Лицензии Лаборатории

Касперского Kaspersky Security Center отображает информацию об этих ключах, а также следующую информацию о комбинации ключа для серверов и ключа для рабочих станций:

- <Уникальная буквенно-цифровая последовательность> – комбинация ключа для серверов и ключа для рабочих станций.
- Срок действия – более длительный из двух сроков использования программы: срок использования программы с ключом для серверов или срок использования программы с ключом для рабочих станций.
- Дата окончания срока годности – более поздняя из двух дат окончания срока годности ключа: дата окончания срока годности ключа для серверов или дата окончания срока годности ключа для рабочих станций.
- Дата окончания срока действия лицензии – более поздняя из двух дат: дата окончания использования программы с ключом для серверов или дата окончания использования программы с ключом для рабочих станций.
- Ограничение – сумма следующих значений: максимальное количество виртуальных машин с операционными системами для рабочих станций и максимальное количество виртуальных машин с операционными системами для серверов, которые вы можете защищать с помощью программы.
- Льготный период – только для ключей по подписке: более длительный из двух льготных периодов: льготный период, соответствующий ключу для серверов, или льготный период, соответствующий ключу для рабочих станций.
- Состояние подписки – только для ключей по подписке: в поле указывается статус Активна, если подписка, соответствующая хотя бы одному из ключей (ключу для серверов или ключу для рабочих станций), находится в статусе "активна". Если обе подписки не активны, в поле указывается лучший статус (например, если одна подписка имеет статус Не активна, а вторая – статус Активирован льготный период, то в поле указывается статус Активирован льготный период).

Просмотр информации о ключе в свойствах программы

Чтобы просмотреть информацию о ключе в свойствах программы, установленной на SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте окно свойств SVM, для которой вы хотите посмотреть информацию о ключе:

a. Выберите группу администрирования, содержащую кластер KSC, в котором находится нужная SVM. b. В

рабочей области выберите закладку Устройства.

c. В списке выберите SVM и откройте окно свойств SVM двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Свойства: <Имя SVM>.

. В окне свойств SVM в списке слева выберите раздел Программы.

В правой части окна отобразится список программ, установленных на этой SVM.

. Выберите программу Kaspersky Kaspersky Security для виртуальных и облачных сред и откройте окно параметров программы двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Параметры программы Kaspersky Kaspersky Security для виртуальных и облачных сред.

. В окне параметров программы в списке слева выберите раздел Ключи.

В правой части окна отобразится информация о ключе, добавленном на SVM. В блоке Активный ключ отображается информация об активном ключе, в блоке Дополнительный ключ отображается информация о дополнительном ключе. Если дополнительный ключ не добавлен, в блоке Дополнительный ключ отображается строка <Не добавлен>.

В блоке Активный ключ отображается следующая информация о ключе:

- <Уникальная буквенно-цифровая последовательность> (ключ).
- Тип лицензии – тип лицензии. Возможные варианты: пробная, коммерческая или подписка.
- Дата активации – дата активации программы путем добавления этого ключа.
- Дата окончания срока действия лицензии – дата окончания срока использования программы, активированной путем добавления этого ключа. Если вы используете программу по неограниченной подписке, в поле отображается Неограниченная.
- Срок действия – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа (например, 365 дней). Если вы используете программу по подписке, в поле отображается <Недоступно>.
- Ограничение – в зависимости от типа ключа:
  - Для ключа для серверов – максимальное количество виртуальных машин с операционной системой для серверов, которые вы можете защищать.
  - Для ключа для рабочих станций – максимальное количество виртуальных машин с операционной системой для рабочих станций, которые вы можете защищать.

    Для ключа для серверов и ключа для рабочих станций при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены. Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин.

  - Для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
  - Для ключа с ограничением по процессорам – максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

В блоке Дополнительный ключ отображается следующая информация о ключе:

- <Уникальная буквенно-цифровая последовательность> (ключ).
- Тип лицензии – тип лицензии: коммерческая.
- Срок действия – количество дней, в течение которых возможно использование программы, активированной путем добавления этого ключа (например, 365 дней).
- Ограничение – в зависимости от типа ключа:
  - Для ключа для серверов – максимальное количество виртуальных машин с операционной системой для серверов, которые вы можете защищать.
  - Для ключа для рабочих станций – максимальное количество виртуальных машин с операционной системой для рабочих станций, которые вы можете защищать.

    Для ключа для серверов и ключа для рабочих станций при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены. Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин.

  - Для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
  - Для ключа с ограничением по процессорам – максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

Если на SVM добавлены и ключ для серверов, и ключ для рабочих станций, то в окне свойств программы Kaspersky Security Center отображает следующую информацию о комбинации ключа для серверов и ключа для рабочих станций:

- <Уникальная буквенно-цифровая последовательность> – комбинация ключа для серверов и ключа для рабочих станций.
- Дата окончания срока действия лицензии – более поздняя из двух дат: дата окончания использования программы с ключом для серверов или дата окончания использования программы с ключом для рабочих станций.
- Срок действия – более длительный из двух сроков использования программы: срок использования программы с ключом для серверов или срок использования программы с ключом для рабочих станций.
- Ограничение – сумма следующих значений: максимальное количество виртуальных машин с операционными системами для рабочих станций и максимальное количество виртуальных машин с операционными системами для серверов, которые вы можете защищать с помощью программы.

Просмотр информации о ключе в свойствах задачи активации программы

Чтобы просмотреть информацию о ключе в свойствах задачи активации программы, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выполните одно из следующих действий:

- Если вы хотите посмотреть свойства задачи активации, которая активирует программу на всех SVM, выберите папку Управляемые устройства дерева консоли. В рабочей области выберите закладку Задачи.
- Если вы хотите посмотреть свойства задачи активации, которая активирует программу на SVM одного кластера KSC, в папке Управляемые устройства дерева консоли выберите группу администрирования, содержащую этот кластер KSC. В рабочей области выберите закладку Задачи.
- Если вы хотите посмотреть свойства задачи активации, которая активирует программу на одной или нескольких SVM, выберите папку Задачи дерева консоли.

. В списке задач выберите задачу активации, свойства которой вы хотите посмотреть, и откройте окно свойств задачи двойным щелчком мыши или выбрав в контекстном меню задачи пункт Свойства.

Откроется окно Свойства: <Название задачи>.

. В окне свойств задачи выберите раздел Добавление лицензионного ключа.

В правой части окна отобразится информация о ключе, добавляемом на SVM с помощью этой задачи:

- Лицензионный ключ – уникальная буквенно-цифровая последовательность.
- Тип лицензии – возможные варианты: пробная, коммерческая или коммерческая (подписка).
- Ограничение – в зависимости от типа ключа:
  - Для ключа для серверов – максимальное количество виртуальных машин с операционной системой для серверов, которые вы можете защищать.
  - Для ключа для рабочих станций – максимальное количество виртуальных машин с операционной системой для рабочих станций, которые вы можете защищать.

    Для ключа для серверов и ключа для рабочих станций при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены. Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин.

  - Для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
  - Для ключа с ограничением по процессорам – максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
- Срок действия лицензии – срок использования программы, указанный в Лицензионном сертификате (например, 365 дней). Поле не отображается, если вы используете программу по подписке.
- Дата окончания срока годности – дата окончания срока годности ключа. Активировать программу путем добавления этого ключа и использовать программу можно только до истечения этого срока. Если вы используете программу по неограниченной подписке, в поле отображается Не определена.

- Льготный период – количество дней после приостановки подписки, в течение которых программа продолжает выполнять все свои функции. Поле отображается, если вы используете программу по подписке и поставщик услуг, у которого вы зарегистрировали подписку, предоставляет льготный период для продления подписки.

- Функциональность – список компонентов и функций программы, доступность которых зависит от вида лицензии, связанной с выбранным ключом:

  - Компоненты и функции программы, доступные при использовании программы по лицензии, соответствующей выбранному ключу, отмечены в списке значком ✔.

  - Компоненты и функции программы, недоступные при использовании программы по лицензии, соответствующей выбранному ключу, отмечены в списке значком ✖.

Просмотр отчета об использовании ключей

Чтобы просмотреть отчет об использовании ключей, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. В рабочей области узла перейдите на закладку Отчеты.

. В списке шаблонов отчетов выберите шаблон Отчет об использовании ключей и откройте окно отчета двойным щелчком мыши или выбрав пункт Показать отчет в контекстном меню.

Откроется окно отчета, сформированного по шаблону Отчет об использовании ключей.

На диаграмме в верхней части окна для каждого ключа отображаются следующие сведения об использовании ключа: количество

- единиц лицензирования, для которых ключ уже используется;

- количество единиц лицензирования, для которых ключ может использоваться в соответствии с лицензионным ограничением;

- количество единиц лицензирования, на которое превышено лицензионное ограничение при использовании ключа.

Отчет об использовании ключей состоит из двух таблиц:

- таблица сводной информации содержит сведения об используемых ключах;

- таблица детальной информации содержит сведения об SVM, на которые добавлены ключи, и о виртуальных машинах, для защиты которых используется ключ.

Вы можете настроить состав полей, отображаемых в каждой таблице. О добавлении и удалении полей в таблицах отчета см. в документации Kaspersky Security Center.

Таблица сводной информации содержит следующие сведения об используемых ключах:

- Ключ – уникальная буквенно-цифровая последовательность.

- Используется всего в качестве активного – в зависимости от типа ключа:

- Для ключа для серверов и ключа для рабочих станций – количество виртуальных машин, для защиты которых используется ключ.
- Для ключа с ограничением по ядрам – количество используемых ядер физических процессоров на всех гипервизорах VMware ESXi, на которых развернуты SVM.
- Для ключа с ограничением по процессорам – количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.

- Используется всего в качестве активного для рабочих станций – количество виртуальных машин с операционными системами для рабочих станций, для защиты которых используется ключ.
- Используется всего в качестве активного для серверов – количество виртуальных машин с операционными системами для серверов, для защиты которых используется ключ.
- Используется всего в качестве дополнительного – количество SVM, на которые ключ добавлен в качестве дополнительного.
- Ограничение – в зависимости от типа ключа:
  - Для ключа для серверов – максимальное количество виртуальных машин с операционной системой для серверов, которые вы можете защищать.
  - Для ключа для рабочих станций – максимальное количество виртуальных машин с операционной системой для рабочих станций, которые вы можете защищать.

  Для ключа для серверов и ключа для рабочих станций при подсчете лицензионных ограничений учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены. Если вы хотите, чтобы виртуальная машина не учитывалась при подсчете лицензионных ограничений, вы можете исключить виртуальную машину из числа защищаемых виртуальных машин.

  - Для ключа с ограничением по ядрам – максимальное количество используемых ядер физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
  - Для ключа с ограничением по процессорам – максимальное количество используемых физических процессоров на всех гипервизорах, виртуальные машины которых вы можете защищать.
- Ближайшая дата окончания срока действия лицензии – дата окончания срока использования программы, активированной путем добавления этого ключа.
- Ключ можно использовать до – дата окончания срока годности ключа.
- Дополнительные свойства – дополнительные свойства ключа.
- Служебная информация – служебная информация, связанная с ключом и лицензией.

В строке ниже находится следующая сводная информация:

- Ключей – общее количество используемых ключей.

- Ключей, используемых более чем на 90% – общее количество ключей, которые используются более чем на 90% от лицензионного ограничения. Например, в ограничении указано 100 виртуальных машин. Ключ используется на двух SVM, из которых первая защищает 42 виртуальных машины, а вторая – 53 виртуальных машины. Следовательно, этот ключ используется на 95% и включен в число ключей, указанное в этом поле.

- Ключей с превышенным ограничением – общее количество ключей, для которых превышено лицензионное ограничение, например, на количество защищаемых виртуальных машин с операционными системами для серверов или с операционными системами для рабочих станций или на количество используемых ядер физических процессоров на всех гипервизорах (в зависимости от типа ключа).

В таблице детальной информации отображаются сведения об SVM, на которую добавлен ключ (для ключей всех типов) и сведения о защищенной виртуальной машине, для которой используется ключ (для ключа для серверов или ключа для рабочих станций):

- Группа – группа администрирования, в которую входит SVM с добавленным ключом.

- Устройство – имя SVM, на которую добавлен ключ, или имя защищенной виртуальной машины, для которой используется ключ.

- Программа – название программы, активированной путем добавления этого ключа на SVM.

- Номер версии – номер версии программы, активированной путем добавления этого ключа на SVM.
- Активный ключ – ключ, который добавлен в качестве активного на SVM или используется для защиты виртуальной машины.

- Дополнительный ключ – ключ, который добавлен в качестве дополнительного на SVM.
- Лицензия действует до – дата окончания использования программы с этим ключом.
- Ключ можно использовать до – дата окончания срока годности ключа.
- IP-адрес – IP-адрес SVM, на которую добавлен ключ, или IP-адрес защищенной виртуальной машины.
- Последнее появление в сети – дата и время, когда SVM или виртуальная машина была видна в локальной сети организации последний раз.

- Последнее соединение с Сервером администрирования – дата и время последнего соединения SVM с Сервером администрирования Kaspersky Security Center.

- NetBIOS-имя – имя защищенной виртуальной машины и путь к ней в виртуальной инфраструктуре.

- DNS-имя – доменное имя SVM или имя защищенной виртуальной машины и путь к ней в виртуальной инфраструктуре.

- Использовано – в зависимости от типа ключа:

  - Для ключа для серверов и ключа для рабочих станций – количество виртуальных машин с операционными системами для серверов или с операционными системами для рабочих станций, которые находятся под защитой программы.

- Для ключа с ограничением по ядрам – количество используемых ядер физических процессоров на всех гипервизорах, на которых развернуты SVM.

- Для ключа с ограничением по процессорам – количество используемых физических процессоров на всех гипервизорах, на которых развернуты SVM.

- Использовано для рабочих станций – количество виртуальных машин с операционными системами для рабочих станций, которые находятся под защитой программы.

- Использовано для серверов – количество виртуальных машин с операционными системами для серверов, которые находятся под защитой программы.

Если на SVM добавлены и ключ для серверов, и ключ для рабочих станций, то в отчете об использовании ключей Kaspersky Security Center отображает следующую информацию о комбинации ключа для серверов и ключа для рабочих станций:

- Ключ, Активный ключ, Дополнительный ключ – уникальная комбинация ключа для серверов и ключа для рабочих станций.

- Ближайшая дата истечения срока действия ключа – более поздняя из двух дат: дата окончания использования программы с ключом для серверов или дата окончания использования программы с ключом для рабочих станций.

- Ключ можно использовать до – более поздняя из двух дат окончания срока годности ключа: дата окончания срока годности ключа для серверов или дата окончания срока годности ключа для рабочих станций.

- Используется всего в качестве активного – общее количество виртуальных машин с операционными системами для серверов и с операционными системами и для рабочих станций, для защиты которых используется ключ.

- Ограничение – сумма следующих значений: максимальное количество защищаемых виртуальных машин с операционными системами для рабочих станций и максимальное количество защищаемых виртуальных машин с операционными системами для серверов.

- Использовано – общее количество виртуальных машин с операционными системами для серверов и с операционными системами для рабочих станций, которые находятся под защитой программы.

Запуск и остановка программы

Kaspersky Security запускается автоматически при запуске операционной системы на SVM.

Функция защиты виртуальных машин от файловых угроз включается автоматически при запуске Kaspersky Security, если вы активировали программу и включили защиту в политике.

Kaspersky Security защищает виртуальные машины от сетевых угроз, только если на SVM применяется политика, в которой настроены параметры предотвращения вторжений и проверки веб-адресов.

Программа не защищает виртуальные машины, если на SVM отсутствуют базы программы.

Задача проверки виртуальных машин запускается в соответствии со своим расписанием.

Kaspersky Security останавливается автоматически при завершении работы операционной системы на SVM.

Состояние защиты

Информация о состоянии защиты виртуальной инфраструктуры в Kaspersky Security Center отображается следующими способами:

- С помощью статуса клиентского устройства (ОК, Критический, Предупреждение). В случае программы Kaspersky Kaspersky Security для виртуальных и облачных сред клиентским устройством Kaspersky Security Center является SVM. Защищенные виртуальные машины не являются клиентскими устройствами с точки зрения Kaspersky Security Center, так как на них не устанавливается Агент администрирования Kaspersky Security Center. При обнаружении проблем в работе программы Kaspersky Security или проблем в защите виртуальных машин изменяется статус той SVM, которая защищает эти виртуальные машины.

  Статус клиентского устройства Kaspersky Security Center может изменяться на Критический или Предупреждение по следующим причинам:

  - Статус изменяется в соответствии с правилами, определенными в Kaspersky Security Center. Например, статус изменяется, если на устройстве не установлена программа защиты, давно не выполнялся поиск вирусов, устарели антивирусные базы или истек срок действия лицензии. Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в документации Kaspersky Security Center.

  - Kaspersky Security Center получает статус устройства от управляемой программы, то есть от Kaspersky Security.

    > В Kaspersky Security Center должно быть включено получение статуса устройства от управляемой программы: в свойствах папки Управляемые устройства в разделе Статус устройства должны быть установлены флажки Определяемый программой в списках условий для статусов Критический и Предупреждение.

  Kaspersky Security может изменять статус SVM на Критический или Предупреждение в следующих случаях:

  - Программа не активирована или обнаружены проблемы, связанные с ключом или лицензией (например, ключ находится в черном списке).

  - Отсутствует подключение SVM к Серверу интеграции или возникли проблемы при получении информации о защищаемой виртуальная инфраструктуре.

  - Обнаружены проблемы и ограничения в работе KSN (произошла ошибка при подключении к KSN, временно ограничено взаимодействие с KSN, параметры KSN в политике не соответствуют параметрам KSN в свойствах Сервера администрирования Kaspersky Security Center).

  - Отсутствуют базы программы или при загрузке баз произошла ошибка.

  - Обнаружены ошибки в работе компонентов программы (например, не выполняется антивирусная проверка, обнаружены ошибки в работе функции обнаружения сетевых атак или обнаружения подозрительной сетевой активности, не выполняется проверка веб-адресов).

  - Обнаружены проблемы взаимодействия SVM с сетевым хранилищем данных (если для SVM настроено использование сетевого хранилища данных).

Подробно о статусах клиентского устройства см. в документации Kaspersky Security Center. Сведения о статусах клиентского устройства (SVM) вы можете посмотреть в списке устройств в Консоли администрирования Kaspersky Security Center и в отчете о состоянии защиты.

- С помощью статуса защиты виртуальных машин. Сведения о статусе защиты виртуальных машин вы можете посмотреть в отчете о состоянии защиты.

  Защищенные виртуальные машины не являются клиентскими устройствами Kaspersky Security Center, поэтому им не может быть назначен статус клиентского устройства. В отчете указывается статус защиты, который Kaspersky Security Center назначает виртуальной машине на основе сведений, полученных от SVM, под защитой которой находится виртуальная машина.

  Статус защиты виртуальной машины может быть изменен на Критический или Предупреждение, если от SVM получена следующая информация:

  - Виртуальная машина находится в статусе "не защищена". Информацию о статусе виртуальной машины (защищена, не защищена, выключена) вы можете посмотреть в списке виртуальных машин в составе защищаемой инфраструктуры кластера KSC.
  - На виртуальной машине давно не выполнялась антивирусная проверка.
  - На SVM, под защитой которой находится виртуальная машина, давно не обновлялись базы программы.

О тегах безопасности (Security Tags)

Kaspersky Security может назначать защищаемой виртуальной машине следующие теги безопасности (Security Tags):

- ANTI_VIRUS.VirusFound.threat=high. Тег назначается виртуальной машине, на которой обнаружены вирусы или другие вредоносные программы.
- IDS_IPS.threat=high. Тег назначается виртуальной машине, в трафике которой обнаружена активность, характерная для сетевых атак, или активность, которая может быть признаком вторжения в защищаемую инфраструктуру.

Вы можете посмотреть теги безопасности, назначенные виртуальной машине, в свойствах виртуальной машины в консоли VMware vSphere Web Client (в разделе Hosts and Clusters на закладке Summary).

Тег безопасности ANTI_VIRUS.VirusFound.threat=high снимается автоматически, если при выполнении задачи проверки на виртуальной машине не обнаружены вирусы или другие вредоносные программы. Тег безопасности IDS_IPS.threat=high можно снять вручную.

Вы можете назначать и снимать теги безопасности вручную (см. подробнее в Базе знаний).

Просмотр информации о виртуальных машинах в составе защищаемой инфраструктуры кластера KSC

Чтобы просмотреть список виртуальных машин в составе защищаемой инфраструктуры кластера KSC, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center в папке Управляемые устройства выберите группу администрирования, содержащую кластер KSC, затем выберите вложенную папку Кластеры и массивы серверов.

. В рабочей области выберите кластер KSC и двойным щелчком мыши откройте окно Свойства: <Название кластера KSC>.

. В окне свойств кластера KSC выберите раздел Список виртуальных машин.

В правой части окна отображается список всех виртуальных машин, которые находятся в составе защищаемой инфраструктуры этого кластера KSC.

В списке не отображаются шаблоны виртуальных машин и SVM.

Список виртуальных машин представлен в виде таблицы, которая содержит следующие графы:

- Статус
- Имя VM
- Путь к VM

. Чтобы посмотреть дополнительную информацию о виртуальных машинах в составе защищаемой инфраструктуры кластера KSC, нажмите на кнопку Детальная информация. В отдельном окне откроется таблица с детальным списком виртуальных машин.

В таблице отображается информация о состоянии защиты, которая указана в поле Тип защиты, расположенном над таблицей. Вы можете выбрать одно из следующих значений:

- Защита файловой системы. Выберите этот вариант, если вы хотите посмотреть информацию о состоянии защиты виртуальных машин от файловых угроз. Этот вариант выбран по умолчанию.
- Сетевая защита. Выберите этот вариант, если вы хотите посмотреть информацию о состоянии сетевой защиты виртуальных машин.

В графах таблицы отображаются следующие дополнительные сведения о каждой виртуальной машине:

- Статус
- Клиент
- Политика безопасности NSX
- Доступные функции защиты
- Тип ОС
- Профиль защиты
- Тип ключа
- Обновление баз
- Дата проверки

В основном и детальном списках виртуальных машин вы можете выполнять следующие действия:

- сортировать список по любой графе таблицы; фильтровать список по статусу защиты;
- выполнять поиск виртуальной машины в списке; экспортировать список виртуальных машин в
- файл в формате XML или в формате CSV.
- Основной и детальный списки виртуальных машин автоматически обновляются каждые пять минут. Если требуется, вы можете обновить список в любой момент с помощью кнопки Обновить список.

Чтобы отфильтровать список виртуальных машин по статусу защиты, нажмите на

одну из следующих кнопок:

-  – показать защищенные виртуальные машины;
-  – показать незащищенные виртуальные машины;
-  – показать выключенные и приостановленные виртуальные машины.

Вы можете комбинировать условия фильтрации, нажав на несколько кнопок.

Чтобы отменить фильтрацию списка виртуальных машин, нажмите на кнопку  .

Чтобы выполнить поиск виртуальной машины в списке,

введите в строке поиска условие поиска виртуальной машины.

В основном списке виртуальных машин вы можете выполнить поиск по значению любой графы, кроме графы Статус. В детальном списке виртуальных машин вы можете выполнить поиск по значению любой графы, кроме граф Статус, Дата проверки и Обновление баз.

Чтобы экспортировать список виртуальных машин в файл в формате XML или в формате CSV, нажмите на кнопку Экспортировать список. В открывшемся окне укажите имя и формат файла.

Информация о виртуальных машинах, которые находятся в составе защищаемой инфраструктуры этого кластера KSC, будет сохранена в файле в выбранном формате.

Если предварительно вы отфильтровали список виртуальных машин или выполнили поиск виртуальной машины, в файле сохраняется только информация, которая соответствует условиям фильтрации или условиям поиска.

Просмотр информации о виртуальных машинах, находящихся под защитой SVM

В свойствах программы, установленной на каждой SVM, вы можете просмотреть информацию о виртуальных машинах, которые находятся под защитой этой SVM.

Виртуальная машина находится под защитой SVM, если установлено соединение между SVM и драйвером Guest Introspection (NSX File Introspection Driver), установленным на виртуальной машине. При этом защита виртуальной машины может быть выключена. SVM с компонентом Защита от файловых угроз защищает только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин от файловых угроз. SVM с компонентом Защита от сетевых угроз защищает только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин от сетевых угроз.

Чтобы просмотреть информацию о виртуальных машинах, которые находятся под защитой SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте окно свойств SVM следующим образом:

a. Выберите группу администрирования, содержащую кластер KSC, в котором находится нужная SVM. b. В рабочей области выберите закладку Устройства.

c. В списке выберите SVM и откройте окно свойств SVM двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Свойства: <Имя SVM>.

. В окне свойств SVM в списке слева выберите раздел Программы.

В правой части окна отобразится список программ, установленных на этой SVM.

. Выберите программу Kaspersky Kaspersky Security для виртуальных и облачных сред и откройте окно параметров программы двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Параметры программы Kaspersky Kaspersky Security для виртуальных и облачных сред.

. В окне параметров программы в списке слева выберите раздел Список защищенных виртуальных машин.

В правой части окна отобразится таблица, содержащая информацию о виртуальных машинах, которые находятся под защитой SVM.

В таблице для каждой виртуальной машины отображаются следующие сведения.

- Имя виртуальной машины.
- Название организации-клиента, которой принадлежит виртуальная машина. Если виртуальная машина не принадлежит ни одной из организаций-клиентов, в графе отображается Нет.
- IP-адрес виртуальной машины.
- Версия операционной системы, установленной на виртуальной машине.
- Тип операционной системы, установленной на виртуальной машине: операционная система для серверов или операционная система для рабочих станций.
- Идентификатор виртуальной машины (vmID).
- Путь к виртуальной машине в виртуальной инфраструктуре.

В таблице со списком виртуальных машин вы можете выполнять следующие действия:

- сортировать список по любой графе таблицы; выполнять поиск виртуальной машины
- в списке; обновлять информацию о виртуальных машинах с помощью кнопки
- Обновить.

Защита виртуальных машин от файловых угроз

Под SVM в этом разделе понимается SVM с установленным компонентом Защита от файловых угроз.

SVM с установленным компонентом Защита от файловых угроз обеспечивает защиту виртуальных машин на гипервизоре VMware ESXi. Параметры, которые SVM применяют во время защиты виртуальных машин от файловых угроз, задаются с помощью политик. Kaspersky Security начинает защищать виртуальные машины только после того, как вы включили защиту с помощью политики.

Защита виртуальных машин от файловых угроз включена, если этим виртуальным машинами назначен профиль защиты. Вы можете назначить основной профиль защиты, который формируется автоматически при создании политики, или создать и назначить дополнительные профили защиты, если вы хотите использовать разные параметры защиты для разных объектов виртуальной инфраструктуры.

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

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

Kaspersky Security защищает только включенные виртуальные машины, для которых выполняются все условия защиты виртуальных машин.

Когда пользователь или программа обращается к файлу виртуальной машины, Kaspersky Security проверяет этот файл.

- Если в файле не обнаружены вирусы или другие вредоносные программы, Kaspersky Security разрешает доступ к этому файлу.

- Если в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус Зараженный. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или другим вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус Зараженный.

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

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

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

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

Уровень эвристического анализа зависит от выбранного уровня безопасности:

- Если установлен уровень безопасности Низкий, применяется поверхностный уровень эвристического анализа. Эвристический анализатор выполняет не все инструкции исполняемых файлов во время проверки исполняемых файлов на наличие вредоносного кода. При таком уровне эвристического анализа вероятность обнаружить угрозу снижена по сравнению со средним уровнем эвристического анализа. Проверка требует меньше ресурсов SVM и проходит быстрее.

- Если установлен уровень безопасности Рекомендуемый, Высокий или Пользовательский, применяется средний уровень эвристического анализа. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет то количество инструкций в исполняемых файлах, которое рекомендовано специалистами "Лаборатории Касперского".

Информация обо всех событиях, произошедших во время защиты виртуальных машин, записывается в отчет.

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 об угрозах 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 защиты, назначенного виртуальным машинам, или временно выключить защиту этих виртуальных машин.

Условия защиты виртуальных машин от файловых угроз

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

- Виртуальная машина не выключена и не приостановлена.

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

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

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

Настройка параметров основного профиля защиты

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

Чтобы настроить параметры основного профиля защиты, выполните следующие действия:

. В блоке Уровень безопасности выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины:

- Если вы хотите установить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его с помощью ползунка.

- Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.

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

a. В блоке Проверка архивов и составных файлов укажите значения следующих параметров:
   - Проверять архивы
   - Удалять архивы, если лечение не удалось
   - Проверять самораспаковывающиеся архивы
   - Проверять вложенные OLE-объекты
   - Не распаковывать составные файлы большого размера
   - Максимальный размер проверяемого составного файла N МБ

b. В блоке Производительность укажите значения следующих параметров:
   - Ограничивать время проверки файлов
   - Проверять файлы не дольше N секунд(ы)

c. В блоке Объекты для обнаружения нажмите на кнопку Настройка и укажите в открывшемся окне Объекты для обнаружения значения следующих параметров:
   - Вредоносные утилиты
   - Программы автодозвона
   - Рекламные программы
   - Другие
   - Многократно упакованные файлы

   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.

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

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

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

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

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

В открывшемся окне Исключения из защиты укажите следующие параметры:

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

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

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

Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

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

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

По умолчанию список исключений содержит объекты, рекомендуемые корпорацией Microsoft (список рекомендуемых исключений см. на сайте корпорации Microsoft). Kaspersky Security исключает эти объекты из защиты на всех

виртуальных машинах, которым назначен основной профиль защиты. Вы можете просмотреть и изменить список этих объектов в таблице Папки и файлы.

Вы можете исключать из защиты объекты следующих типов:

- Папки. Из защиты исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение из защиты к вложенным папкам.

- Файлы по маске. Из защиты исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

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

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

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

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

. Нажмите на кнопку ОК в окне Исключения из защиты.

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания политики) или на кнопку Применить (в свойствах политики).

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

Управление дополнительными профилями защиты

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

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

. В Консоли администрирования Kaspersky Security Center откройте свойства политики:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

c. В списке политик выберите политику и двойным щелчком мыши по политике откройте окно Свойства:

<Название политики>.

. В окне свойств политики в разделе Защита от файловых угроз выберите подраздел Дополнительные профили защиты.

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

В списке дополнительных профилей защиты вы можете выполнять следующие действия:

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

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

Создание дополнительного профиля защиты

Чтобы создать дополнительный профиль защиты, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте список дополнительных профилей защиты в свойствах политики, для которой вы хотите создать дополнительный профиль защиты.

. Нажмите на кнопку Добавить.

Откроется окно Профиль защиты.

. В открывшемся окне введите имя нового профиля защиты.

Имя профиля защиты не может содержать более 255 символов.

. Если при создании нового профиля защиты вы хотите использовать ранее сохраненные параметры профиля защиты, установите флажок Импортировать параметры из файла и укажите путь к файлу в формате JSON.

. Нажмите на кнопку ОК в окне Профиль защиты.

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

Параметры дополнительного профиля защиты, кроме списка исключений по умолчанию, аналогичны параметрам основного профиля защиты.

> 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.

. После настройки всех параметров профиля защиты нажмите на кнопку ОК в окне Параметры защиты.
В окне Свойства: <Название политики> в списке дополнительных профилей защиты отобразится новый профиль защиты.

Созданные дополнительные профили вы можете назначать виртуальным машинам или другим объектам виртуальной инфраструктуры VMware, а также устанавливать соответствия между профилями защиты и конфигурациями профилей NSX (NSX Profile Configurations).

Просмотр защищаемой инфраструктуры в политике

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

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

. В Консоли администрирования Kaspersky Security Center откройте свойства политики:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от файловых угроз выберите подраздел Защищаемая инфраструктура.

. Плагин управления Kaspersky Security пытается автоматически подключиться к Серверу интеграции. Если установить подключение не удалось, откроется окно Подключение к Серверу интеграции.

Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции по умолчанию используется ваша доменная учетная запись. Флажок Использовать доменную учетную запись установлен по умолчанию. Вы также можете использовать учетную запись

администратора Сервера интеграции (admin). Для этого снимите флажок Использовать доменную учетную запись и введите пароль администратора в поле Пароль.

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

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

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

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

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

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

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

- Использовать дерево виртуальной инфраструктуры. Если выбран этот вариант, в таблице отображается дерево объектов виртуальной инфраструктуры VMware и профили защиты, назначенные объектам виртуальной инфраструктуры.

- Использовать конфигурации профилей NSX (NSX Profile Configurations). Если выбран этот вариант, в таблице отображаются конфигурации профилей NSX (NSX Profile Configurations), доступные для выбранного сервера VMware vCenter Server, и соответствующие им профили защиты.

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

Информация о назначении параметров файловой защиты с использованием дерева виртуальной инфраструктуры

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

Защищаемая инфраструктура отображается в виде дерева элементов:

- В свойствах политики для одного сервера VMware vCenter Server отображается защищаемая инфраструктура кластера "VMware vCenter Agentless": корневым элементом является сервер VMware vCenter Server, под ним расположены объекты Datacenter, кластеры VMware, ресурсные пулы, объекты vApp и виртуальные машины. Kaspersky Security использует отображение защищаемой инфраструктуры кластера KSC в виде дерева гипервизоров VMware ESXi и кластеров VMware (Hosts and Clusters view) (см. подробнее в документации к продуктам VMware).

- В свойствах политики для всей защищаемой инфраструктуры корневым элементом является Сервер интеграции, под ним расположены все серверы VMware vCenter Server, каждый из них содержит защищаемую инфраструктуру кластера "VMware vCenter Agentless", соответствующего этому серверу VMware vCenter Server.

- В свойствах политики для клиентов, размещенной в папке Управляемые устройства виртуального Сервера администрирования, корневым элементом является условный объект "Организация vCloud Director", который объединяет все виртуальные Datacenter клиента. Под ним расположены все виртуальные машины, входящие в состав организации vCloud Director, которая соответствует этому виртуальному Серверу администрирования.

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

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

Графа Профиль защиты может содержать следующие значения:

- Имя профиля защиты, назначенного виртуальной машине или объекту виртуальной инфраструктуры VMware.

- Имя профиля защиты, унаследованного от родительского объекта, в виде "унаследованный: <N>", где <N> – имя унаследованного профиля защиты.

- (Не назначен) или унаследованный: (Не назначен) – если профиль защиты не назначался или назначение профиля защиты было отменено (выбрано значение Не использовать профиль защиты). Виртуальные машины или объекты виртуальной инфраструктуры, которым не назначен профиль защиты, исключаются из защиты.

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

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

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

  В качестве профиля защиты по умолчанию выбран основной профиль защиты. Если вы отменили использование профиля защиты по умолчанию, в строке отображается значение Не использовать профиль защиты.

- Таблица соответствий между конфигурациями профилей NSX, доступными для выбранного сервера VMware vCenter Server, и профилями защиты.

В таблице отображаются следующие сведения:

- Графа Конфигурация профиля NSX содержит имя конфигурации профиля NSX (NSX Profile Configuration). Если в виртуальной инфраструктуре создано несколько конфигураций профилей NSX с одинаковым идентификатором (Configuration ID), их имена отображаются через запятую. Конфигурации профилей NSX с одинаковыми идентификаторами программа Kaspersky Security обрабатывает как одну и ту же конфигурацию профиля NSX.

- Если соответствие между конфигурацией профиля NSX и профилем защиты установлено, в графе Профиль защиты отображается имя профиля защиты. Для защиты виртуальных машин, на которые распространяется действие этой конфигурации профиля NSX, Kaspersky Security использует параметры указанного профиля защиты.

- Если соответствие было отменено, в графе Профиль защиты отображается значение (Не назначен). Если конфигурации профиля NSX не соответствует никакой профиль защиты, виртуальные машины, на которые распространяется действие этой конфигурации профиля NSX, исключаются из защиты.

Назначение профилей защиты объектам виртуальной инфраструктуры

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

. В свойствах политики, в области действия которой находятся нужные виртуальные машины или другие объекты виртуальной инфраструктуры VMware, выберите подраздел Защищаемая инфраструктура.

. Если вы настраиваете политику для одного сервера VMware vCenter Server, убедитесь, что в раскрывающемся списке, расположенном в верхней части окна, выбран вариант Использовать дерево виртуальной инфраструктуры. Это значение выбрано по умолчанию.

. Выберите один или несколько объектов виртуальной инфраструктуры в таблице.

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

. Нажмите на кнопку Выбрать профиль защиты.

Откроется окно Выбор профиля защиты.

. Выберите один из следующих вариантов:

- Наследовать родительский профиль защиты: <имя>. Выберите этот вариант, чтобы назначить виртуальной машине или другому объекту виртуальной инфраструктуры профиль защиты родительского объекта.
- Использовать профиль защиты. Выберите этот вариант и укажите в раскрывающемся списке имя профиля защиты, чтобы назначить этот профиль защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.

. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, профиль защиты назначается объекту и всем его дочерним объектам, включая объекты, которым назначен собственный профиль защиты или которые исключены из защиты. Если вы хотите назначить профиль защиты только выбранному объекту виртуальной инфраструктуры и тем его дочерним объектам, которым не назначен собственный профиль защиты и которые не исключены из защиты, снимите флажок Применить ко всем дочерним объектам.

. Нажмите на кнопку ОК.

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

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

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

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

. В консоли VMware vSphere Web Client:

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

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

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

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

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

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

. В свойствах политики для одного сервера VMware vCenter Server выберите подраздел Защищаемая инфраструктура.

. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант Использовать конфигурации профилей NSX (NSX Profile Configurations).

. В таблице выберите конфигурацию профиля NSX, для которой вы хотите установить соответствие, и двойным щелчком мыши откройте окно Выбор профиля защиты.

. В открывшемся окне выберите вариант Использовать профиль защиты и укажите в раскрывающемся списке имя профиля защиты, который должен соответствовать конфигурации профиля NSX. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.

. Нажмите на кнопку ОК.

Окно Выбор профиля защиты закроется, установленное соответствие отобразится в таблице в подразделе Защищаемая инфраструктура.

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

Конфигурациям профилей NSX, для которых еще не устанавливалось соответствие с профилем защиты, или соответствие было отменено в результате удаления профиля защиты, автоматически назначается профиль защиты по умолчанию. Вы можете изменить профиль защиты по умолчанию или отменить использование профиля защиты по умолчанию.

Чтобы изменить профиль защиты по умолчанию, выполните следующие действия:

. В свойствах политики для одного сервера VMware vCenter Server выберите подраздел Защищаемая инфраструктура.

. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант Использовать конфигурации профилей NSX (NSX Profile Configurations).

. Нажмите на кнопку Изменить, расположенную справа от названия профиля защиты по умолчанию.

Откроется окно Выбор профиля защиты.

. Если вы хотите изменить профиль защиты по умолчанию, выберите вариант Использовать профиль защиты и укажите в раскрывающемся списке имя профиля защиты. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.

Указанный профиль защиты будет соответствовать конфигурациям профилей NSX, для которых соответствие с профилем защиты еще не устанавливалось, или соответствие было отменено в результате удаления профиля защиты.

. Если вы хотите отменить использование профиля защиты по умолчанию, выберите вариант Не использовать профиль защиты. Конфигурациям профилей NSX, для которых соответствие с профилем защиты еще не устанавливалось, или соответствие было отменено в результате удаления профиля защиты, по умолчанию не будет соответствовать никакой профиль защиты. Виртуальные машины, находящиеся под действием этих конфигураций профилей NSX, будут исключены из защиты.

. Нажмите на кнопку ОК.

Окно Выбор профиля защиты закроется, в верхней части окна в подразделе Защищаемая инфраструктура отобразится имя выбранного профиля защиты.

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

Изменение защищаемой инфраструктуры для политики

Вы можете изменить защищаемую инфраструктуру, выбранную для политики. Это может потребоваться, например, если вы хотите скопировать политику из одной группы администрирования в другую. В этом случае вам нужно изменить для скопированной политики защищаемую инфраструктуру так, чтобы защищаемая инфраструктура соответствовала расположению политики:

- если политика расположена в группе, которая содержит кластер "VMware vCenter Agentless", в качестве защищаемой инфраструктуры для политики должен быть выбран сервер VMware vCenter Server, соответствующий этому кластеру;
- если политика расположена в папке Управляемые устройства или в группе, которая содержит кластер "VMware vCloud Director Agentless", в качестве защищаемой инфраструктуры для политики должна быть выбрана вся защищаемая инфраструктура.

Чтобы изменить защищаемую инфраструктуру, выбранную для политики, выполните следующие действия:

. В свойствах политики, защищаемую инфраструктуру которой вы хотите изменить, выберите подраздел Защищаемая инфраструктура.

. В правой части окна нажмите на кнопку Изменить.

. Откроется окно Подключение к Серверу интеграции. В окне отображаются параметры подключения к тому Серверу интеграции, адрес которого указан в нижней части окна. Если требуется, измените параметры подключения и нажмите на кнопку ОК.

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

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

  Если выбранный VMware vCenter Server не соответствует кластеру "VMware vCenter Agentless", в группе которого расположена политика, Kaspersky Security не защищает виртуальные машины.

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

. Нажмите на кнопку ОК в окне Выбор защищаемой инфраструктуры и подтвердите в открывшемся окне изменение защищаемой инфраструктуры.

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

Выключение защиты объектов виртуальной инфраструктуры от файловых угроз

Вы можете выключить защиту объектов виртуальной инфраструктуры от файловых угроз следующими способами:

- Если параметры файловой защиты заданы путем назначения профилей защиты объектам виртуальной инфраструктуры, вы можете отменить назначение профиля защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Виртуальные машины, которым не назначен профиль защиты, исключаются из защиты.

- Если параметры файловой защиты заданы с использованием конфигураций профилей NSX (NSX Profile Configurations), вы можете отменить соответствие между профилем защиты и конфигурацией профиля NSX, действие которой распространяется на виртуальные машины. Если конфигурации профиля NSX не соответствует никакой профиль защиты, виртуальные машины, на которые распространяется действие этой конфигурации профиля NSX, исключаются из защиты.

- Вы можете выключить защиту для всех виртуальных машин, которые находятся в области действия политики.

Если параметры файловой защиты заданы путем назначения профилей защиты объектам виртуальной инфраструктуры, чтобы выключить защиту для одной или нескольких виртуальных машин, выполните следующие действия:

. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел Защищаемая инфраструктура.

. Если вы настраиваете политику для одного сервера VMware vCenter Server, убедитесь, что в раскрывающемся списке, расположенном в верхней части окна, выбран вариант Использовать дерево виртуальной инфраструктуры.

. Выберите один или несколько объектов виртуальной инфраструктуры в графе Имя.

Если вы хотите выключить защиту для нескольких виртуальных машин, которые являются дочерними объектами одного объекта виртуальной инфраструктуры, выберите этот объект. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.

. Нажмите на кнопку Выбрать профиль защиты.

Откроется окно Выбор профиля защиты.

. Выберите вариант Не использовать профиль защиты.

. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, по умолчанию защита будет выключена для выбранного объекта и для всех его дочерних объектов, включая объекты, которым назначен собственный профиль защиты. Если вы хотите выключить защиту только для выбранного объекта виртуальной инфраструктуры и тех его дочерних объектов, которые наследуют профиль защиты, снимите флажок Применить ко всем дочерним объектам.

Защита будет снята с родительского объекта и тех его дочерних объектов, у которых профиль защиты унаследован от родительского объекта. Под защитой программы останутся дочерние объекты, которым назначен собственный профиль защиты.

. Нажмите на кнопку ОК.

Окно Выбор профиля защиты закроется, в таблице в подразделе Защищаемая инфраструктура для объектов, которые исключены из защиты, в графе Профиль защиты отобразится значение (Не назначен).

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

Если параметры файловой защиты заданы с использованием конфигураций профилей NSX, чтобы выключить защиту виртуальных машин, выполните следующие действия:

. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел Защищаемая инфраструктура.
. В раскрывающемся списке, расположенном в верхней части окна, выберите вариант Использовать конфигурации профилей NSX (NSX Profile Configurations).

. В таблице выберите конфигурацию профиля NSX, действие которой распространяется на нужные виртуальные машины, и двойным щелчком мыши откройте окно Выбор профиля защиты.

. В открывшемся окне выберите вариант Не использовать профиль защиты.

. Нажмите на кнопку ОК.

Окно Выбор профиля защиты закроется, в таблице в подразделе Защищаемая инфраструктура для выбранной конфигурации профиля NSX в графе Профиль защиты отобразится значение (Не назначен).

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

Чтобы выключить защиту для всех виртуальных машин, которые находятся в области действия политики, выполните следующие действия:

. В свойствах политики, в области действия которой находятся нужные виртуальные машины, выберите подраздел Защищаемая инфраструктура.

. Снимите флажок Использовать защиту от файловых угроз, расположенный в верхней части окна.

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

Проверка виртуальных машин

Под SVM в этом разделе понимается SVM с установленным компонентом Защита от файловых угроз.

SVM с установленным компонентом Защита от файловых угроз позволяет выполнять антивирусную проверку файлов виртуальных машин на гипервизоре VMware ESXi. Требуется периодически проверять файлы виртуальных машин с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов.

Параметры, которые SVM применяют во время проверки виртуальных машин, задаются с помощью задач проверки. Kaspersky Security использует для проверки следующие задачи:

- Полная проверка. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин, находящихся в области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

  Задача полной проверки автоматически создается после установки основного плагина управления Kaspersky Security в папке Управляемые устройства главного Сервера администрирования Kaspersky Security Center. Эта задача позволяет выполнять антивирусную проверку всех виртуальных машин, которые находятся под защитой всех SVM и не входят в организации vCloud Director. Вы можете запускать эту задачу вручную.

- Выборочная проверка. Задача позволяет выполнять антивирусную проверку файлов указанных виртуальных машин из области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу. В рамках выбранной области действия вам нужно указать виртуальные машины, которые требуется проверять. Вы можете указывать отдельные виртуальные машины, объекты виртуальной инфраструктуры VMware более высокого уровня иерархии или группы безопасности NSX (NSX Security Group), в которые входят нужные виртуальные машины.

Вы можете запускать задачи проверки вручную, задавать расписание выполнения задач проверки и просматривать информацию о ходе и результатах выполнения задач.

Kaspersky Security проверяет только виртуальные машины, для которых выполняются все условия проверки виртуальных машин.

Если во время проверки файлов виртуальных машин в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус Зараженный. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус Зараженный.

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

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

Во время проверки виртуальных машин всегда используется глубокий уровень эвристического анализа независимо от выбранного уровня безопасности. Эвристический анализатор выполняет максимальное количество инструкций в исполняемых файлах, что позволяет повысить вероятность обнаружения угрозы.

> Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из области проверки.

Особенности проверки виртуальных машин:

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

- При выполнении задач проверки Kaspersky Security может проверять шаблоны виртуальных машин.

- При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется настроить задачу проверки для виртуальных машин, на которых открыт сетевой доступ к папкам и файлам, и включить эти папки и файлы в область проверки задачи.

  При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

- Во время выполнения задачи проверки одна SVM с установленным компонентом Защита от файловых угроз одновременно проверяет файлы не более четырех виртуальных машин.

Информация о результатах проверки и обо всех событиях, произошедших во время выполнения задач проверки, записывается в отчет.

После завершения задачи проверки рекомендуется просмотреть список файлов, заблокированных в результате выполнения задачи, и вручную выполнить действия с этими файлами. Например, сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Предварительно требуется исключить заблокированные файлы из защиты в параметрах профиля защиты, назначенного виртуальным машинам, или временно выключить защиту виртуальных машин, на которых были заблокированы эти файлы. Информацию о заблокированных файлах вы можете просмотреть в отчете об угрозах или в выборке событий по событию Файл
заблокирован (см. в документации Kaspersky Security Center).

Условия антивирусной проверки виртуальных машин

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

- Для выключенных виртуальных машин: на виртуальной машине используется файловая система NTFS, FAT32, EXT2, EXT3, EXT4, XFS или BTRFS.

- Для включенных виртуальных машин:

  - на виртуальной машине установлен и запущен драйвер Guest Introspection (NSX File Introspection Driver).

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

    Выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS программа Kaspersky Security может проверять в соответствии с параметрами проверки независимо от того, входят ли эти виртуальные машины в состав группы безопасности NSX (NSX Security Group).

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

Kaspersky Security также не проверяет виртуальную машину, если выполняется одно из следующих условий:

- Вы добавили виртуальную машину в список объектов виртуальной инфраструктуры (Inventory) в консоли VMware vSphere Web Client или создали виртуальную машину на гипервизоре VMware ESXi после того, как была запущена задача проверки.
- Вы удалили виртуальную машину из списка объектов виртуальной инфраструктуры (Inventory) в консоли VMware vSphere Web Client до начала проверки этой виртуальной машины.
- Виртуальная машина, входящая в область действия запущенной задачи проверки, мигрирует на гипервизор VMware ESXi, на котором не запущена задача проверки.

Создание задачи полной проверки

Чтобы создать задачу полной проверки, выполните следующие действия:

.

В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой вы хотите создать задачу.

Если вы выбрали папку Управляемые устройства или группу администрирования, содержащую кластер KSC, в рабочей области выберите закладку Задачи.

. Нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите тип задачи.

- Если вы хотите создать задачу для проверки виртуальных машин, которые не входят в организации vCloud Director, выберите Kaspersky Kaspersky Security для виртуальных и облачных сред ⟶ Полная проверка.
- Если вы хотите создать задачу для проверки виртуальных машин клиентов, выберите Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) ⟶ Полная проверка.

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры проверки виртуальных машин.

Перейдите к следующему шагу мастера создания задачи.

. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи.

Перейдите к следующему шагу мастера создания задачи.

. Если вы запустили мастер создания задачи из папки Задачи, укажите способ выбора SVM, на которых должна выполняться задача:

- Нажмите на кнопку Выбрать устройства, обнаруженные в сети Сервером администрирования, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
- Нажмите на кнопку Задать адреса устройств вручную или импортировать из списка, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

  Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку Назначить задачу выборке устройств, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.
- Нажмите на кнопку Назначить задачу группе администрирования, если задача должна выполняться на всех SVM, входящих в группу администрирования.

В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

- В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.
- Нажмите на кнопку Добавить или Добавить IP-диапазон и задайте адреса SVM.
- Нажмите на кнопку Импортировать и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
- Нажмите на кнопку Обзор и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
- Нажмите на кнопку Обзор и выберите группу администрирования или введите название группы администрирования вручную.

Перейдите к следующему шагу мастера создания задачи.

. Настройте расписание запуска задачи и перейдите к следующему шагу мастера.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера.

. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок Запустить задачу после завершения работы мастера.

Завершите работу мастера.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную.

Создание задачи выборочной проверки с помощью основного плагина

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

Чтобы создать задачу выборочной проверки для виртуальных машин, которые не входят в организации vCloud Director, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите группу администрирования, в которой вы хотите создать задачу.

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

.

. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

На первом шаге мастера выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред → Выборочная проверка.

Перейдите к следующему шагу мастера создания задачи.

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

Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен и ваша доменная учетная запись входит в группу KLAdmins или в группу локальных администраторов на компьютере, где установлен Сервер интеграции, для подключения к Серверу интеграции по умолчанию используется ваша доменная учетная запись. Флажок Использовать доменную учетную запись установлен по умолчанию.

Если вы хотите использовать учетную запись администратора Сервера интеграции (admin), снимите флажок Использовать доменную учетную запись и введите пароль администратора в поле Пароль.

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

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

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

Перейдите к следующему шагу мастера создания задачи.

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

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

После того, как подключение будет установлено, откроется окно Список серверов VMware vCenter Server. Выберите VMware vCenter Server, под управлением которого находятся виртуальные машины, которые вы хотите проверять, и нажмите на кнопку ОК.

. На этом шаге мастера выберите область действия задачи.

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры проверки виртуальных машин.

Перейдите к следующему шагу мастера создания задачи.

. Если требуется, сформируйте область проверки для задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи.

Перейдите к следующему шагу мастера создания задачи.

. Настройте расписание запуска задачи и перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера 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.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную.

В случае замены / переустановки сервера VMware vCenter Server все ранее созданные задачи выборочной проверки перестают работать. Если вы хотите использовать ранее созданную задачу выборочной проверки, вам требуется выполнить повторное подключение к серверу VMware vCenter Server в свойствах этой задачи.

Создание задачи выборочной проверки с помощью плагина для клиентов

Задача выборочной проверки для виртуальных машин клиентов используется, только если программа работает в режиме multitenancy. Создание задачи выборочной проверки для виртуальных машин клиентов поддерживается только на виртуальном Сервере администрирования Kaspersky Security Center

Чтобы создать задачу выборочной проверки для виртуальных машин клиентов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства виртуального Сервера администрирования, соответствующего клиенту.

.

. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

На первом шаге мастера выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) → Выборочная проверка.

Перейдите к следующему шагу мастера создания задачи.

. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера создания задачи.

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

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

. Выберите область действия задачи: установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

> Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры проверки виртуальных машин.

Перейдите к следующему шагу мастера создания задачи.

. Если требуется, сформируйте область проверки для задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи.

Перейдите к следующему шагу мастера создания задачи.

. Настройте расписание запуска задачи и перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера 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.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную.

Настройка параметров проверки виртуальных машин в задаче проверки

Вы можете настроить параметры проверки виртуальных машин во время создания задачи (шаг Настройка параметров проверки) или в свойствах задачи после ее создания (раздел Параметры проверки).

Чтобы настроить параметры проверки виртуальных машин, выполните следующие действия:

. Выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины. Для этого в блоке Уровень безопасности выполните одно из следующих действий:

- Если вы хотите установить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его с помощью ползунка.
- Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.
- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку Настройка. В открывшемся окне Параметры уровня безопасности выполните следующие действия:

a. В блоке Проверка архивов и составных файлов укажите значения следующих параметров:
   - Проверять архивы
   - Удалять архивы, если лечение не удалось
   - Проверять самораспаковывающиеся архивы
   - Проверять вложенные OLE-объекты
   - Не распаковывать составные файлы большого размера
   - Максимальный размер проверяемого составного файла N МБ

b. В блоке Производительность укажите значения следующих параметров:
   - Ограничивать время проверки файлов
   - Проверять файлы не дольше N секунд(ы)

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

.

- Вредоносные утилиты
- Программы автодозвона Рекламные
- программы

- Другие
- Многократно упакованные файлы

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.

. В блоке Проверка включенных виртуальных машин настройте параметры проверки виртуальных машин, которые включены во время выполнения задачи:

- Действие при обнаружении угрозы
- Проверять оптические диски

. В блоке Проверка выключенных виртуальных машин и шаблонов виртуальных машин настройте параметры проверки виртуальных машин, которые выключены или приостановлены во время выполнения задачи, а также шаблонов виртуальных машин:

- Проверять выключенные виртуальные машины
- Проверять шаблоны виртуальных машин
- Действие при обнаружении угрозы

. В блоке Останавливать проверку выберите один из следующих вариантов:

- По истечении N минут(ы) с момента запуска задачи
- После окончания проверки файлов на всех защищенных виртуальных машинах

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Настройка области проверки в задаче проверки

Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Если область проверки не настроена, Kaspersky Security проверяет все файлы виртуальных машин.

При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется

создать задачу проверки виртуальных машин, папки и файлы которых открыты для сетевого доступа, и включить эти папки и файлы в область проверки задачи.

При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

Вы можете сформировать область проверки задачи во время создания задачи (шаг Выбор области проверки) или в свойствах задачи после ее создания (раздел Область проверки).

Чтобы настроить область проверки задачи, выполните следующие действия:

. 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, вы можете сформировать список объектов, которые требуется исключить из области проверки, с помощью кнопок Добавить, Изменить и Удалить.

Вы можете исключать из области проверки объекты следующих типов:

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

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

  Kaspersky Security не учитывает регистр символов в путях к файлам и папкам, именах и масках файлов, которые требуется исключить из области проверки.

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

В комплект поставки программы входит файл microsoft_file_exclusions.xml, который содержит список исключений, рекомендуемых корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Файл microsoft_file_exclusions.xml расположен в папке установки плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Вы можете импортировать этот файл в исключения задачи проверки. После выполнения импорта Kaspersky Security не проверяет объекты, рекомендуемые корпорацией Microsoft, во время выполнения задачи проверки. Вы можете просмотреть и изменить список этих объектов в таблице Папки и файлы.

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

. Если вы выбрали вариант Проверять все папки и файлы, кроме указанных, в блоке Расширения файлов вы можете указать расширения файлов, которые нужно включить в область проверки или исключить из области проверки.

Для этого выберите один из следующих вариантов:

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

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

  Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

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

Исключенные из проверки папки имеют более высокий приоритет, чем расширения файлов, включенные в область проверки. Если файл находится в папке, исключенной из проверки, то программа не проверяет его, несмотря на то, что расширение файла включено в область проверки.

. Если вы выбрали вариант Проверять только указанные папки и файлы, с помощью кнопок Добавить, Изменить и Удалить сформируйте список папок и файлов на виртуальной машине, которые нужно проверять во время выполнения задачи проверки.

При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в путях к файлам и директориям, включаемым в область проверки. При проверке виртуальных машин с операционными системами Windows регистр символов в путях к файлам и папкам не учитывается.

Если в списке объектов, которые нужно проверять, вы используете переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows в область проверки включаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, в область проверки включаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Настройка области действия задачи выборочной проверки

Вы можете настроить область действия задачи выборочной проверки во время создания задачи (шаг Настройка области действия задачи) или в свойствах задачи после ее создания (раздел Область действия задачи).

Задача выборочной проверки, созданная с помощью основного плагина управления

Для задачи выборочной проверки, созданной с помощью основного плагина управления Kaspersky Security, вы можете настроить область действия задачи одним из следующих способов:

- Указать виртуальные машины и / или шаблоны виртуальных машин, файлы которых вы хотите проверить.
- Указать одну или несколько групп безопасности NSX (NSX Security Group), в которые включены виртуальные машины. Kaspersky Security проверит файлы всех виртуальных машин, которые включены в указанные группы безопасности NSX.

Чтобы настроить область действия задачи выборочной проверки, созданной с помощью основного плагина управления, выполните следующие действия:

. Если вы хотите включить в область действия задачи виртуальные машины и / или шаблоны виртуальных машин, в раскрывающемся списке в верхней части окна выберите вариант Объекты виртуальной инфраструктуры (этот вариант выбран по умолчанию). В окне отобразится виртуальная инфраструктура VMware под управлением одного сервера VMware vCenter Server в виде дерева объектов: VMware vCenter Server, объекты Datacenter, кластеры VMware, ресурсные пулы, объекты vApp и виртуальные машины.

   Установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

   > Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

. Если вы хотите включить в область действия задачи все виртуальные машины, входящие в одну или несколько групп безопасности NSX, в раскрывающемся списке в верхней части окна выберите вариант Группы безопасности NSX.

   Установите флажки для групп безопасности NSX, виртуальные машины которых вы хотите проверить во время выполнения создаваемой задачи.

   > Если областью действия задачи является одна или несколько групп безопасности NSX, во время выполнения этой задачи Kaspersky Security не проверяет шаблоны виртуальных машин, даже если в параметрах проверки установлен флажок Проверять шаблоны виртуальных машин.

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Задача выборочной проверки, созданная с помощью плагина управления для клиентов

Для задачи выборочной проверки, созданной с помощью плагина управления Kaspersky Security для клиентов, недоступно формирование области действия задачи с помощью групп безопасности NSX. Вы можете включать в область действия задач отдельные виртуальные машины или их объединения.

Чтобы настроить область действия задачи выборочной проверки, созданной с помощью плагина управления для клиентов, выполните следующие действия:

. Установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

> Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Настройка расписания запуска задач проверки

Вы можете настроить расписание запуска задач проверки во время создания задачи (шаг Настройка расписания запуска задачи) или в свойствах задачи после ее создания (раздел Расписание).

Чтобы настроить расписание запуска задачи, выполните следующие действия:

. Определите значения следующих параметров:

- Запуск по расписанию. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- Запускать пропущенные задачи. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов Вручную и Один раз задача запускается сразу после появления SVM в сети.

  Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов Вручную и Один раз – только на видимых в сети SVM.

- 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.

- Использовать случайную задержку запуска задачи в интервале (мин). Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок Использовать автоматическое определение случайного интервала между запусками задачи.

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

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Защита от сетевых угроз

Под SVM в этом разделе понимается SVM с установленным компонентом Защита от сетевых угроз.

SVM с установленным компонентом Защита от сетевых угроз обеспечивает защиту виртуальных машин на гипервизоре VMware ESXi. Параметры, которые SVM применяют во время защиты виртуальных машин от сетевых угроз, задаются с помощью политик. Kaspersky Security начинает защищать виртуальные машины только после того, как вы настроили параметры защиты от сетевых угроз в активной политике.

Kaspersky Security защищает от сетевых угроз только те виртуальные машины, для которых выполняются все условия защиты виртуальных машин.

Компонент Kaspersky Security Защита от сетевых угроз выполняет следующие функции:

- Предотвращение вторжений. Kaspersky Security позволяет обнаруживать и блокировать в трафике защищенных виртуальных машин активность, характерную для сетевых атак, и подозрительную сетевую активность, которая может быть признаком вторжения в защищаемую инфраструктуру.

  Kaspersky Security может проверять трафик с IP-адресов в формате IPv4 и IPv6.

- Проверка веб-адресов. Kaspersky Security позволяет проверять веб-адреса, к которым обращается пользователь или какая-либо программа, и блокировать доступ к веб-адресам в случае обнаружения угрозы.

Параметры работы компонента Защита от сетевых угроз зависят от режима обработки трафика, выбранного при регистрации службы сетевой защиты:

- Если вы выбрали Стандартный режим, при обнаружении признаков вторжений или попытки доступа к опасным или нежелательным веб-адресам Kaspersky Security выполняет то действие, которое указано в параметрах политики, и передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

- Если вы выбрали Режим мониторинга, при обнаружении признаков вторжений или попытки доступа к опасным или нежелательным веб-адресам Kaspersky Security не предпринимает действий по предотвращению угроз, а только передает информацию о событиях на Сервер администрирования Kaspersky Security Center.

Вы можете выбрать режим обработки трафика только при регистрации службы сетевой защиты (Kaspersky Network Protection).

Вы можете настраивать исключения из защиты от сетевых угроз следующими способами:

- Исключать из проверки входящий или исходящий трафик всех виртуальных машин, которым назначена одна политика безопасности NSX (NSX Security Policy). Вы можете указать, какой трафик следует проверять, в политике безопасности NSX, в которой настроено использование службы сетевой защиты (Kaspersky Network Protection). Настройка политики безопасности NSX (NSX Security Policy) выполняется в консоли VMware vSphere Web Client.

- Формировать правила исключения из защиты от сетевых угроз, в соответствии с которыми Kaspersky Security может исключать из проверки трафик определенных IP-адресов или применять при его обработке особые действия.

Информация о событиях, произошедших во время защиты виртуальных машин от сетевых угроз, передается на Сервер администрирования Kaspersky Security Center и записывается в отчет.

Описания известных в настоящее время видов сетевых атак и признаков вторжений, а также базы вредоносных и фишинговых веб-адресов содержатся в базах программы и пополняются в процессе обновления баз программы.

Условия защиты виртуальных машин от сетевых угроз

Одна SVM с установленным компонентом Защита от сетевых угроз, развернутая на гипервизоре VMware ESXi, обеспечивает защиту всех виртуальных машин на этом гипервизоре, для которых выполняются следующие условия:

- 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 сетевой защиты (Kaspersky Network Protection) и включено перенаправление трафика службе сетевой защиты (параметр Redirect to service).

Компонент Защита от сетевых угроз может проверять исходящий и / или входящий трафик виртуальных машин. Вы можете указать, какой трафик следует проверять, в политике безопасности NSX (NSX Security Policy), в которой настроено использование службы сетевой защиты (Kaspersky Network Protection). Настройка политики безопасности NSX (NSX Security Policy) выполняется в консоли VMware vSphere Web Client.

Предотвращение вторжений

В ходе защиты виртуальных машин от вторжений Kaspersky Security может выполнять следующие действия:

- Обнаруживать сетевые атаки на защищенные виртуальные машины.

  Если обнаружение сетевых атак включено, при обнаружении попытки сетевой атаки на защищенную виртуальную машину Kaspersky Security выполняет действие, заданное в параметрах политики. Например, программа может прервать соединение между виртуальной машиной и IP-адресом, с которого произведена сетевая атака, или прервать соединение и заблокировать трафик с этого IP-адреса, чтобы автоматически защитить виртуальную машину от возможных будущих сетевых атак с этого IP-адреса.

- Обнаруживать в трафике защищенных виртуальных машин подозрительную сетевую активность. Наличие в трафике защищенной виртуальной машины подозрительной сетевой активности может быть признаком вторжения в защищаемую инфраструктуру. При анализе трафика виртуальных машин применяются правила выявления подозрительной сетевой активности, которые содержатся в базах программы Kaspersky Security.

  Если контроль сетевой активности включен, при обнаружении подозрительной сетевой активности Kaspersky Security выполняет действие, заданное в параметрах политики. Например, программа может прервать соединение с IP-адресом, который проявляет подозрительную сетевую активность, или прервать соединение и заблокировать трафик с этого IP-адреса.

Если в соответствии с настроенными параметрами Kaspersky Security блокирует трафик с IP-адреса, который является источником сетевой атаки или подозрительной сетевой активности, то продолжительность блокировки по умолчанию составляет 60 минут. Вы можете изменить продолжительность блокировки трафика. По истечении указанного времени трафик автоматически разблокируется.

> При определении источника сетевой атаки или подозрительной сетевой активности учитывается принадлежность трафика к виртуальной локальной сети (VLAN). Kaspersky Security блокирует трафик с IPадреса только в той виртуальной локальной сети, в которой была обнаружена сетевая атака или подозрительная сетевая активность.

Список источников сетевых угроз, заблокированных в результате работы каждой SVM с компонентом Защита от сетевых угроз, отображается в свойствах программы, установленной на этой SVM. По истечении времени блокировки, заданного в параметрах программы, источник сетевых угроз автоматически удаляется из списка. При необходимости вы можете отменить блокировку трафика с выбранных IP-адресов, не дожидаясь автоматической разблокировки.

Вы можете настроить правила исключения из защиты от сетевых угроз, в соответствии с которыми Kaspersky Security исключает из проверки трафик определенных IP-адресов или применяет особые действия при обработке этого трафика.

При обнаружении сетевой атаки или подозрительной сетевой активности Kaspersky Security назначает тег безопасности IDS_IPS.threat=high виртуальной машине, в трафике которой обнаружена активность, характерная для сетевых атак, или подозрительная сетевая активность.

Включение и выключение функции обнаружения сетевых атак

Чтобы включить или выключить функцию обнаружения сетевых атак, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Предотвращение вторжений.

. Выполните одно из следующих действий:

- Установите флажок Обнаруживать сетевые атаки, если вы хотите, чтобы программа Kaspersky Security обнаруживала в трафике защищенных виртуальных машин активность, характерную для сетевых атак.

  Если флажок установлен, при обнаружении попытки сетевой атаки на защищенную виртуальную машину Kaspersky Security выполняет действие, заданное в параметрах программы. Если сетевая защита развернута в стандартном режиме, по умолчанию Kaspersky Security прерывает соединение между защищенной виртуальной машиной и IP-адресом, с которого произведена сетевая атака, а также блокирует трафик с этого IP-адреса на 60 минут. Вы можете изменить это действие и период блокировки трафика. Если сетевая защита развернута в режиме мониторинга, Kaspersky Security не выполняет никаких действий по предотвращению сетевой атаки.

- Снимите флажок Обнаруживать сетевые атаки, если вы хотите, чтобы программа Kaspersky Security не проверяла трафик защищенных виртуальных машин на наличие активности, характерной для сетевых атак.

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

Настройка параметров обнаружения сетевых атак

Чтобы настроить параметры обнаружения сетевых атак, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Предотвращение вторжений.

. Установите флажок Обнаруживать сетевые атаки, если функция обнаружения сетевых атак выключена.

. Выберите действие в раскрывающемся списке Действие при обнаружении сетевой атаки, если сетевая защита развернута в стандартном режиме.

Если сетевая защита развернута в режиме мониторинга, при обнаружении сетевой атаки Kaspersky Security выполняет действие Игнорировать.

. Если требуется, измените значение параметра При обнаружении угрозы блокировать трафик на N минут.

. Если требуется, настройте правила исключения из защиты от сетевых угроз, в соответствии с которыми Kaspersky Security исключает из проверки трафик с определенных IP-адресов или применяет особые действия при обработке этого трафика.

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

Включение и выключение контроля сетевой активности виртуальных машин

Функция обнаружения подозрительной сетевой активности доступна, только если вы используете программу по расширенной лицензии.

Чтобы включить или выключить контроль сетевой активности виртуальных машин, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Предотвращение вторжений.

. Выполните одно из следующих действий:

- Установите флажок Контролировать сетевую активность виртуальных машин, если вы хотите, чтобы программа Kaspersky Security обнаруживала в трафике защищенных виртуальных машин подозрительную сетевую активность, которая может быть признаком вторжения в защищаемую инфраструктуру.

  Если флажок установлен, при обнаружении в трафике защищенных виртуальных машин подозрительной сетевой активности Kaspersky Security выполняет действие, заданное в параметрах программы. Если сетевая защита развернута в стандартном режиме, по умолчанию Kaspersky Security прерывает соединение между защищенной виртуальной машиной, которая проявляет подозрительную сетевую активность, и другими виртуальными машинами. Вы можете изменить это действие. Если сетевая защита развернута в режиме мониторинга, Kaspersky Security не выполняет никаких действий в отношении виртуальных машин, проявляющих подозрительную сетевую активность.

- Снимите флажок Контролировать сетевую активность виртуальных машин, если вы хотите, чтобы программа Kaspersky Security не проверяла трафик защищенных виртуальных машин на наличие подозрительной сетевой активности.

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

Настройка параметров контроля сетевой активности виртуальных машин

Функция обнаружения подозрительной сетевой активности доступна, только если вы используете программу по расширенной лицензии.

Чтобы настроить параметры контроля сетевой активности защищенных виртуальных машин, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Предотвращение вторжений.

. Установите флажок Контролировать сетевую активность виртуальных машин, если контроль сетевой активности виртуальных машин выключен.

. Нажмите на кнопку Настройка.

Откроется окно Параметры контроля сетевой активности.

. Укажите категории программ, признаки сетевой активности которых должна обнаруживать программа Kaspersky Security:

- Рекламные программы
- Другие программы

Kaspersky Security всегда обнаруживает в трафике защищенных виртуальных машин сетевую активность, характерную для таких вредоносных программ, как вирусы, черви и троянские программы.

. Если Kaspersky Security выявляет сетевую активность, которая, по вашему мнению, не является признаком вторжения в защищаемую инфраструктуру, вы можете настроить список правил, которые Kaspersky Security не будет применять для выявления подозрительной сетевой активности в трафике защищенных виртуальных машин.

Чтобы добавить в список правило, в соответствии с которым обнаруживается сетевая активность, нажмите на кнопку Добавить, расположенную над списком, и введите в строке списка идентификатор правила в следующем формате: `<число>:<число>:<число>`.

Информацию о примененном правиле вы можете посмотреть в тексте события, отправленного в Kaspersky Security Center во время обнаружения подозрительной сетевой активности.

. Нажмите на кнопку ОК в окне Параметры контроля сетевой активности.

. Выберите действие в раскрывающемся списке

Действие при обнаружении подозрительной активности, если сетевая защита развернута в стандартном режиме .

Если сетевая защита развернута в режиме мониторинга, при обнаружении подозрительной сетевой активности Kaspersky Security выполняет действие Игнорировать.

. Если требуется, измените значение параметра При обнаружении угрозы блокировать трафик на N минут .

. Если требуется, настройте правила исключения из защиты от сетевых угроз, в соответствии с которыми Kaspersky Security исключает из проверки трафик с определенных IP-адресов или применяет особые действия при обработке этого трафика.

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

Просмотр списка заблокированных источников сетевых угроз

В свойствах программы, установленной на SVM с компонентом Защита от сетевых угроз, вы можете просмотреть список источников сетевых угроз, заблокированных в результате работы этой SVM.

Чтобы просмотреть список заблокированных источников сетевых угроз на SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте окно свойств SVM:

a. Выберите группу администрирования, содержащую кластер KSC, в котором находится нужная SVM. b. В рабочей

области выберите закладку Устройства.

c. В списке выберите SVM и откройте окно свойств SVM двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Свойства: <Имя SVM>.

. В окне свойств SVM в списке слева выберите раздел Программы.

В правой части окна отобразится список программ, установленных на этой SVM.

. Выберите программу Kaspersky Kaspersky Security для виртуальных и облачных сред и откройте окно параметров программы двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Параметры программы Kaspersky Kaspersky Security для виртуальных и облачных сред.

. В окне параметров программы в списке слева выберите раздел Список заблокированных источников сетевых угроз.

В правой части окна отобразится таблица, содержащая список источников сетевых угроз, заблокированных в результате работы этой SVM, то есть список IP-адресов, трафик с которых программа Kaspersky Security заблокировала в результате обнаружения сетевой атаки или подозрительной сетевой активности.

В таблице для каждого источника сетевых угроз отображается следующая информация:

- IP-адрес – IP-адрес, трафик с которого программа Kaspersky Security заблокировала в результате обнаружения сетевой атаки или подозрительной сетевой активности.
- VLAN ID – идентификатор виртуальной локальной сети (VLAN), к которой относится заблокированный трафик.
- Начало блокировки – дата и время, когда программа Kaspersky Security заблокировала трафик с IP-адреса.
- Окончание блокировки – дата и время, когда трафик с IP-адреса будет автоматически разблокирован.

В списке заблокированных источников сетевых угроз вы можете выполнять следующие действия:

- Выполнять поиск заблокированных источников сетевых угроз по значениям графы IP-адрес. По умолчанию в таблице отображается информация только о последних 100 заблокированных источниках сетевых угроз. Если источник сетевых угроз, информацию о котором вы хотите посмотреть, не отображается в таблице, вы можете воспользоваться поиском. Для этого нужно ввести в поисковой строке IP-адрес, начало IP-адреса или маску подсети и нажать на кнопку Найти. В результате в таблице отображается не более 100 заблокированных источников сетевых угроз, удовлетворяющих условиям поиска.
- Сортировать список по любой графе таблицы. Если поисковый запрос не задан, сортировка выполняется по всему списку заблокированных источников сетевых угроз. Если вы выполнили поиск, сортировка применяется только к списку источников сетевых угроз, которые удовлетворяют условиям поиска.
- Обновлять информацию с помощью кнопки Обновить.

По истечении времени блокировки, заданного в параметрах программы, источник сетевых угроз автоматически удаляется из списка. Если требуется, вы можете отменить блокировку трафика с выбранных IP-адресов, не дожидаясь автоматической разблокировки.

Чтобы разблокировать трафик с IP-адреса, который признан источником сетевых угроз,

выберите один или несколько источников сетевых угроз в списке и нажмите на кнопку Разблокировать, расположенную в нижней части окна.

Проверка веб-адресов

Kaspersky Security может проверять веб-адреса, к которым обращаются по протоколу HTTP пользователь или какаялибо программа, установленная на защищенной виртуальной машине. При проверке веб-адресов Kaspersky Security может использовать базы вредоносных и фишинговых веб-адресов, а также информацию о репутации интернетресурсов, полученную из Глобального KSN.

По умолчанию, если проверка веб-адресов включена, Kaspersky Security проверяет веб-адреса на принадлежность к вредоносным, фишинговым и рекламным веб-адресам. Kaspersky Security также может проверять веб-адреса на принадлежность к категории веб-адресов, связанных с распространением легальных программ, которые могут быть использованы для нанесения вреда виртуальной машине или данным пользователя. Вы можете указать, какие категории веб-адресов должна обнаруживать программа.

Для обнаружения рекламных веб-адресов и веб-адресов, связанных с распространением легальных программ, которые могут быть использованы для нанесения вреда виртуальной машине или данным пользователя, требуется использование Глобального KSN в работе программы Kaspersky Security. Если Глобальный KSN не используется, программа не проверяет веб-адреса на принадлежность к этим категориям веб-адресов.

Если проверка включена, при обнаружении принадлежности веб-адреса к одной или нескольким выбранным категориям веб-адресов, Kaspersky Security выполняет заданное в параметрах программы действие, например блокирует или разрешает доступ к этому веб-адресу.

Если программа Kaspersky Security блокирует доступ к веб-адресу, к которому обращается пользователь, в браузере на защищенной виртуальной машине отображается сообщение о блокировке.

Вы можете сформировать список веб-адресов, доступ к которым Kaspersky Security не блокирует, независимо от действия, заданного в параметрах программы.

Kaspersky Security не проверяет веб-адрес, если к нему происходит обращение с IP-адреса, трафик которого исключен из проверки в соответствии с правилами исключения из защиты от сетевых угроз.

Если вы используете программу в режиме multitenancy, Kaspersky Security проверяет веб-адреса, к которым происходит обращение с виртуальных машин клиентов, только по базам вредоносных и фишинговых вебадресов.

Включение и выключение проверки веб-адресов

Чтобы включить или выключить проверку веб-адресов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Проверка веб-адресов.

. Выполните одно из следующих действий:

- Установите флажок Проверять веб-адреса, если вы хотите, чтобы программа Kaspersky Security проверяла принадлежность веб-адресов, к которым обращается пользователь или какая-либо программа, к категориям веб-адресов, выбранным для обнаружения. По умолчанию Kaspersky Security проверяет веб-адреса на принадлежность к вредоносным, фишинговым и рекламным веб-адресам. Вы можете выбрать категории веб-адресов для обнаружения в окне, которое открывается по кнопке Настройка.

  При обнаружении принадлежности веб-адреса к одной или нескольким выбранным категориям веб-адресов Kaspersky Security по умолчанию блокирует доступ к этому веб-адресу. Вы можете изменить это действие, а также сформировать список веб-адресов, доступ к которым Kaspersky Security не будет блокировать в случае обнаружения угрозы.

- Снимите флажок Проверять веб-адреса, если вы хотите выключить проверку веб-адресов.

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

Настройка параметров проверки веб-адресов

Чтобы настроить параметры проверки веб-адресов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей

области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Проверка веб-адресов.

. Установите флажок Проверять веб-адреса, если проверка веб-адресов выключена.

. Нажмите на кнопку Настройка.

Откроется окно Веб-адреса для обнаружения.

. Укажите категории веб-адресов, которые должна обнаруживать программа Kaspersky Security:

- Вредоносные веб-адреса
- Фишинговые веб-адреса
- Рекламные веб-адреса
- Другие веб-адреса

. Нажмите на кнопку ОК в окне Веб-адреса для обнаружения.

. Выберите действие в раскрывающемся списке Действие при обнаружении угрозы, если сетевая защита развернута в стандартном режиме.

Если сетевая защита развернута в режиме мониторинга, при обнаружении принадлежности веб-адреса к одной или нескольким выбранным категориям Kaspersky Security выполняет действие Игнорировать.

. В таблице Не блокировать доступ к указанным веб-адресам нажмите на кнопку Добавить или на клавишу **INSERT** и введите веб-адрес в графе Веб-адрес .

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

Настройка сообщения о блокировке веб-адреса

В случае блокировки веб-адреса, к которому обращается пользователь, Kaspersky Security отображает сообщение о блокировке в браузере на защищенной виртуальной машине. Вы можете просмотреть пример сообщения о блокировке веб-адреса и выбрать язык сообщения о блокировке.

Чтобы выбрать язык сообщения о блокировке веб-адреса и просмотреть пример сообщения, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Прочее.

. По ссылке Посмотреть пример сообщения откройте пример сообщения о блокировке веб-адреса, которое отображается в браузере на защищенной виртуальной машине.

Пример сообщения открывается в новом окне.

. В блоке Настройка локализации в раскрывающемся списке Язык сообщения о блокировке веб-адреса выберите язык сообщения о блокировке веб-адреса.

По умолчанию выбран язык, соответствующий локализации плагина управления Kaspersky Security.

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

Настройка исключений из защиты от сетевых угроз

В политике вы можете настроить правила исключения из защиты от сетевых угроз, в соответствии с которыми Kaspersky Security исключает из проверки трафик с определенных IP-адресов или применяет особые действия при обработке этого трафика. Вы можете задавать правила исключения как для трафика с отдельных IP-адресов, так и для трафика со всех IP-адресов в IP-подсети. При формировании области действия правил учитывается принадлежность трафика к виртуальной локальной сети (VLAN).

Если группа портов виртуального коммутатора работает в режиме Virtual Switch Tagging (VST), при применении правил исключения к трафику виртуальных машин, относящихся к этой группе портов, не учитывается принадлежность трафика к виртуальной локальной сети (VLAN).

Чтобы настроить правило исключения из защиты от сетевых угроз, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей

области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от сетевых угроз выберите подраздел Исключения из защиты.

. Нажмите на кнопку Добавить или на клавишу **INSERT** и укажите область действия правила исключения в графе Область действия .

. Выберите правило исключения в графе Правило.

. Если требуется, измените положение созданного правила исключения в списке с помощью стрелок, расположенных над списком. Приоритет правила определяется его положением в списке. Если для одной и той же области действия вы задали несколько правил, то в первую очередь применяется правило, расположенное в списке выше.

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

Обновление баз программы

Базы программы содержат описания угроз компьютерной безопасности, которые позволяют обнаруживать в проверяемых объектах вредоносный код, описания известных в настоящее время видов сетевых атак и признаков вторжений, а также базы вредоносных и фишинговых веб-адресов.

Обновление баз программы обеспечивает актуальность защиты виртуальных машин. Каждый день в мире появляются новые вирусы и другие вредоносные программы. Чтобы программа Kaspersky Security своевременно обнаруживала угрозы, вам нужно регулярно обновлять базы программы.

Для обновления баз 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 обновления баз программы. Задача позволяет распространять и устанавливать обновления баз программы на SVM сразу после загрузки пакета обновлений в хранилище Сервера администрирования.

Настройка автоматического обновления баз программы

Чтобы настроить автоматическое обновление баз программы, выполните следующие действия:

. Убедитесь, что в Kaspersky Security Center создана задача загрузки обновлений в хранилище.

Задача загрузки обновлений в хранилище создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Если задача загрузки обновлений в хранилище была удалена из списка задач Сервера администрирования, вы можете создать новую задачу. См. подробнее в документации Kaspersky Security Center.

. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы.

Задача обновления баз программы может быть создана автоматически после установки основного плагина управления Kaspersky Security. Вы можете использовать эту задачу для обновления баз программы.

Если задача отсутствует, создайте ее.

Задача обновления баз программы запускается по расписанию. Вы можете посмотреть результаты ее выполнения и при необходимости запустить задачу вручную.

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 антивирусных баз.

Создание задачи обновления баз программы

Чтобы создать задачу обновления баз программы, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой вы хотите создать задачу.

Если вы выбрали папку Управляемые устройства или группу администрирования, содержащую кластер KSC, в рабочей области выберите закладку Задачи.

. Нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред → Обновление. Перейдите к следующему шагу мастера создания задачи.

. Если вы запустили мастер создания задачи из папки Задачи, укажите способ выбора SVM, на которых должна выполняться задача:

- Нажмите на кнопку Выбрать устройства, обнаруженные в сети Сервером администрирования, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.

- Нажмите на кнопку Задать адреса устройств вручную или импортировать из списка, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

  Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку Назначить задачу выборке устройств, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.

- Нажмите на кнопку Назначить задачу группе администрирования, если задача должна выполняться на всех SVM, входящих в группу администрирования.

  В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

  - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.
  - Нажмите на кнопку Добавить или Добавить IP-диапазон и задайте адреса SVM.
  - Нажмите на кнопку Импортировать и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
  - Нажмите на кнопку Обзор и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
  - Нажмите на кнопку Обзор и выберите группу администрирования или введите название группы администрирования вручную.

  Перейдите к следующему шагу мастера создания задачи.

. В поле Запуск по расписанию выберите При загрузке обновлений в хранилище. 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.

. В поле Имя введите название задачи обновления баз программы и перейдите к следующему шагу мастера 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 отката обновления 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.

После установки или обновления программы Kaspersky Security SVM передают в Kaspersky Security Center информацию о том, какие базы требуются для работы программы. 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
(см. подробнее в документации Kaspersky Security Center), дождаться ее выполнения, а затем вручную запустить задачу обновления 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:

. Создайте задачу отката обновления. Вы можете создать задачу для всех SVM, для SVM одного кластера KSC или для отдельной SVM.

. Запустите задачу отката обновления.

Создание задачи отката обновления

Чтобы создать задачу отката обновления, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой вы хотите создать задачу.

Если вы выбрали папку Управляемые устройства или группу администрирования, содержащую кластер KSC, в рабочей области выберите закладку Задачи.

. Нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред → Откат обновления. Перейдите к следующему шагу мастера создания задачи.

. Если вы запустили мастер создания задачи из папки Задачи, укажите способ выбора SVM, на которых должна выполняться задача:

- Нажмите на кнопку Выбрать устройства, обнаруженные в сети Сервером администрирования, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.
- Нажмите на кнопку Задать адреса устройств вручную или импортировать из списка, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

  Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку Назначить задачу выборке устройств, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.

- Нажмите на кнопку Назначить задачу группе администрирования, если задача должна выполняться на всех SVM, входящих в группу администрирования.

  В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

  - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.
  - Нажмите на кнопку Добавить или Добавить IP-диапазон и задайте адреса SVM.
  - Нажмите на кнопку Импортировать и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
  - Нажмите на кнопку Обзор и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
  - Нажмите на кнопку Обзор и выберите группу администрирования или введите название группы администрирования вручную.

  Перейдите к следующему шагу мастера создания задачи.

. 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.

. В поле Имя введите название задачи отката обновления и перейдите к следующему шагу мастера 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 отката обновления отобразится в списке задач.

Резервное хранилище

Под SVM в этом разделе понимается SVM с установленным компонентом Защита от файловых угроз.

Резервное хранилище – это специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

Резервная копия файла – копия файла с виртуальной машины, которая создается при лечении или удалении этого файла. Резервные копии файлов хранятся в резервном хранилище в специальном формате и не представляют опасности.

Когда программа Kaspersky Security обнаруживает зараженный файл на виртуальной машине, она закрывает пользователю виртуальной машины доступ к этому файлу, а затем помещает его копию в резервное хранилище. Далее программа выполняет над файлом то действие, которое указано в профиле защиты этой виртуальной машины, например лечит или удаляет файл. Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал информацию, которая в результате лечения стала полностью или частично недоступна, вы можете сохранить файл из резервной копии на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Резервное хранилище располагается на SVM с установленным компонентом Защита от файловых угроз. По умолчанию на каждой SVM включено использование резервного хранилища.

> При удалении или обновлении SVM с компонентом Защита от файловых угроз копии файлов, помещенные в резервное хранилище на SVM, автоматически удаляются.

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 указываются в параметрах политики.

Вы можете работать с резервными копиями файлов, которые находятся в резервных хранилищах на SVM, в Консоли администрирования Kaspersky Security Center. В Консоли администрирования Kaspersky Security Center представлен общий список резервных копий файлов, помещенных программой Kaspersky Security в резервное хранилище на каждой SVM с установленным компонентом Защита от файловых угроз.

Чтобы избежать удаления резервных копий файлов в результате удаления или обновления SVM, вы можете настроить использование сетевого хранилища данных для SVM. Если использование сетевого хранилища данных включено, резервные копии файлов с каждой SVM сохраняются в отдельной папке в сетевом хранилище данных. SVM подключается к хранилищу каждые 10 минут для синхронизации данных. Если резервные копии на SVM были удалены автоматически в результате удаления или обновления SVM, они будут автоматически восстановлены. Если вы удалили резервные копии файлов на SVM вручную, эти копии также удаляются из папки в сетевом хранилище данных. Срок хранения резервных копий файлов в сетевом хранилище данных определяется параметрами резервного хранилища на SVM.

Вы можете настроить использование сетевого хранилища данных для SVM во время установки программы (процедура регистрации служб Kaspersky Security) или с помощью процедуры изменения параметров Kaspersky Security.

Настройка параметров резервного хранилища

Чтобы настроить параметры резервного хранилища на SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Резервное хранилище.

. В правой части окна укажите следующие параметры:

- Помещать файлы в резервное хранилище.

  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.

- Хранить файлы не более N 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.

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

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.

Просмотр списка резервных копий файлов

Чтобы просмотреть список резервных копий файлов,

в Консоли администрирования Kaspersky Security Center в папке Дополнительно → Хранилища выберите папку Резервное хранилище.

В рабочей области отобразится список резервных копий файлов, помещенных в резервные хранилища на всех SVM.

Список резервных копий файлов представлен в виде таблицы. Каждая строка таблицы содержит событие, произошедшее с зараженным файлом, и информацию об обнаруженном в файле объекте.

В графах таблицы отображается следующая информация:

- Устройство – имя и путь к виртуальной машине, на которой обнаружен файл.
- Имя – имя файла.
- Статус – статус, который программа Kaspersky Security присвоила обнаруженному файлу после обработки: Удален, Вылечен.

Выполняемое действие – действие, которое на текущий момент выполняет программа с этой резервной копией файла в резервном хранилище. Например, если вы дали команду удалить резервную копию файла, то в этой графе отображается Удаляется. Если программа не выполняет действий над этой резервной копией файла, то это поле пусто.

- Дата помещения – дата и время помещения резервной копии файла в резервное хранилище.
- Объект – название объекта, обнаруженного в файле. Если в файле обнаружено несколько объектов, то в списке резервных копий файлов каждый обнаруженный объект отображается на отдельной строке.
- Размер – размер файла в байтах.
- Папка восстановления – полный путь к исходному файлу на виртуальной машине.
- Описание – имя виртуальной машины и полный путь на ней к исходному файлу, резервная копия которого помещена в резервное хранилище.

Сохранение файлов из резервного хранилища на диск

Вы можете сохранить файлы из резервного хранилища на жесткий диск компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Чтобы сохранить файл из резервного хранилища на диск, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center в папке Дополнительно → Хранилища выберите папку Резервное хранилище.

В рабочей области отобразится список резервных копий файлов, помещенных в резервные хранилища на всех SVM.

. В списке резервных копий файлов выберите файл, который вы хотите сохранить на диск.

. 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.

. Выберите папку на жестком диске компьютера, в которую вы хотите сохранить файл.

. 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.

Удаление резервных копий файлов

Чтобы удалить резервные копии файлов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center в папке Дополнительно → Хранилища выберите папку Резервное хранилище.

В рабочей области отобразится список резервных копий файлов, помещенных в резервные хранилища на всех SVM.

. В списке резервных копий файлов выберите файлы, которые вы хотите удалить. Используйте клавиши **CTRL** и **SHIFT**, чтобы выбрать несколько файлов.

. 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.

События, уведомления и отчеты

Вы можете получать сведения о работе Kaspersky Security в Kaspersky Security Center с помощью следующих средств:

- отчеты; уведомления о
- событиях; статистика.
- SVM отправляют на Сервер администрирования Kaspersky Security Center служебные сообщения с информацией о работе Kaspersky Security – события. Информация о событиях сохраняется в базе данных Сервера администрирования.

Выделяют следующие уровни важности событий:

- Критическое событие. Событие критической важности, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке. Может указывать на проблемы в работе Kaspersky Security или на уязвимости в защите виртуальных машин.
- Отказ функционирования. Событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- Предупреждение. Событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky Security и может указывать на возможную проблему в будущем.

Информационное сообщение. Событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

Уведомление – это сообщение с информацией о событии, которое произошло на SVM. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе программы. Kaspersky Security Center позволяет выбирать способ уведомления о событиях и настраивать параметры уведомлений о событиях в свойствах политики.

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

На основе событий Kaspersky Security Center формирует различные типы отчетов. С помощью отчетов вы можете получить, например, сведения о зараженных файлах, изменении параметров защиты, использовании лицензионных ключей и баз программы. Вы можете просматривать отчеты в Консоли администрирования Kaspersky Security Center.

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

Настройка параметров уведомлений

Чтобы настроить параметры уведомлений о событиях, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей

области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Настройка событий.

. Выберите закладку с названием уровня важности событий, о которых вы хотите получать уведомления:

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

. Выберите типы событий, о которых вы хотите получать уведомления:

- Используйте клавиши **SHIFT** и **CTRL**, если вы хотите выбрать несколько типов событий.
-

-

Нажмите на кнопку Выбрать все, если вы хотите выбрать все типы событий.

. Нажмите на кнопку Свойства.

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

. 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.

. В блоке Уведомления о событиях выберите способ уведомления:

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

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

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

Типы отчетов

С помощью отчетов вы можете получать информацию о работе Kaspersky Security: сведения о развертывании защиты, о состоянии защиты, о выполнении запущенных задач, об обнаруженных угрозах.

Kaspersky Security Center предоставляет набор отчетов, в которых содержится информация о работе Kaspersky Security:

- Отчет о версиях программ "Лаборатории Касперского". Содержит сведения о версиях программ, установленных на клиентских устройствах (SVM и компьютере, на котором установлены Сервер администрирования и Консоль администрирования Kaspersky Security Center).
- Отчет о развертывании защиты. Содержит сведения о развертывании компонентов программы.
- Отчет о наиболее заражаемых устройствах. Содержит информацию о виртуальных машинах, в ходе проверки которых обнаружено наибольшее количество зараженных файлов.
- Отчет об угрозах. Содержит информацию о вирусах и вредоносных программах, обнаруженных на виртуальных машинах, а также информацию о действиях, которые программа Kaspersky Security выполнила над файлами, в которых обнаружены угрозы.
- Отчет об использовании ключей. Содержит информацию о лицензионных ключах, добавленных в программу.
- Отчет об ошибках. Содержит информацию об ошибках, возникших в работе программы.
- Отчет об используемых базах. Содержит информацию о версиях и состоянии баз программы, используемых на SVM.

- Отчет о сетевых атаках. Содержит информацию о зарегистрированных сетевых атаках на виртуальные машины и о подозрительной сетевой активности, обнаруженной в трафике защищенных виртуальных машин компонентом Защита от сетевых угроз.

  Отчет о работе Веб-Контроля. Содержит информацию об обращениях пользователей или программ к опасным и нежелательным веб-адресам, зафиксированных компонентом Защита от сетевых угроз.

- Отчет о состоянии защиты. Содержит сведения о состоянии защиты виртуальных машин.

Для программы Kaspersky Security не поддерживается отчет о реестре оборудования. Сведения об оборудовании SVM вы можете посмотреть в консоли VMware vSphere Web Client.

Каждый отчет состоит из таблицы сводной информации и таблицы детальной информации. Вы можете настроить состав полей, отображаемых в каждой таблице.

В этой справке описана работа с отчетами Kaspersky Security Center 11.

Для получения более подробной информации о работе с отчетами см. в документации Kaspersky Security Center.

Отчет о версиях программ Лаборатории Касперского

Отчет о версиях программ "Лаборатории Касперского" содержит сведения о версиях компонентов Kaspersky Security, установленных на SVM, и версиях компонентов Kaspersky Security Center, установленных на клиентских устройствах (SVM и устройствах, на которых установлен Сервер администрирования Kaspersky Security Center и / или Агент администрирования Kaspersky Security Center).

Отчет содержит следующую сводную информацию:

- Программа – название установленного компонента Kaspersky Security или компонента Kaspersky Security Center. Для компонентов Kaspersky Security в поле указывается Kaspersky Kaspersky Security для виртуальных и облачных сред или Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов).

- Номер версии – номер версии установленного компонента Kaspersky Security или компонента Kaspersky Security Center.

- Количество устройств – для компонентов Kaspersky Security отображается количество SVM, на которых установлены компоненты Kaspersky Security; для программы Kaspersky Security Center – количество устройств, на которых установлены Сервер администрирования и / или Агент администрирования Kaspersky Security Center.

- Количество групп – для компонентов Kaspersky Security отображается количество групп администрирования, в которые входят SVM; для программы Kaspersky Security Center – количество групп администрирования, в которые входят устройства с установленными Сервером администрирования и / или Агентом администрирования Kaspersky Security Center.

  В строке ниже находится следующая сводная информация:

- Всего программ – общее количество различных версий компонентов Kaspersky Security и компонентов Kaspersky Security Center, установленных на клиентских устройствах.
- Количество установок – общее количество установок этих компонентов на клиентских устройствах.
- Количество устройств – общее количество клиентских устройств, на которых установлены компоненты Kaspersky Security и компоненты Kaspersky Security Center.

–

- Количество групп общее количество групп администрирования, в которые входят эти клиентские устройства.

Отчет содержит следующую детальную информацию:

- Программа – название установленного компонента Kaspersky Security или компонента Kaspersky Security Center. Для компонентов Kaspersky Security в поле указывается Kaspersky Kaspersky Security для виртуальных и облачных сред или Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов).

- Номер версии – номер версии установленного компонента Kaspersky Security или компонента Kaspersky Security Center.

- Группа – для компонентов Kaspersky Security отображается название группы администрирования, в которую входит SVM с установленным компонентом Kaspersky Security; для программы Kaspersky Security Center – название группы администрирования, в которую входит устройство с установленными Сервером администрирования и / или Агентом администрирования Kaspersky Security Center.

- Устройство – для компонентов Kaspersky Security отображается имя SVM, на которой установлен компонент; для компонентов Kaspersky Security Center – имя устройства, на котором установлены Сервер администрирования и / или Агент администрирования Kaspersky Security Center.

- Установлено – дата и время установки компонента Kaspersky Security или компонента Kaspersky Security Center на клиентское устройство.

- Последнее появление в сети – дата и время, когда клиентское устройство появлялось в локальной сети организации последний раз.

- Последнее соединение с Сервером администрирования – дата и время последнего соединения клиентского устройства с Сервером администрирования Kaspersky Security Center.

- IP-адрес – для компонентов Kaspersky Security отображается IP-адрес SVM, на которой установлен компонент; для компонентов Kaspersky Security Center – IP-адрес устройства, на котором установлены Сервер администрирования и / или Агент администрирования Kaspersky Security Center.

- DNS-имя – для компонентов Kaspersky Security отображается доменное имя SVM, на которой установлен компонент; для компонентов Kaspersky Security Center – имя устройства, на котором установлены Сервер администрирования и / или Агент администрирования Kaspersky Security Center.

Отчет о развертывании защиты

Отчет о развертывании защиты содержит сведения об установленных компонентах защиты "Лаборатории Касперского" на клиентских устройствах Kaspersky Security Center (SVM и компьютере, на котором установлен Агент администрирования Kaspersky Security Center).

Отчет содержит следующую сводную информацию:

- Компоненты защиты – возможные варианты установки компонентов и программ "Лаборатории Касперского" на клиентских устройствах:

- –
  - Установлен Агент администрирования и антивирусная защита.
  - Установлен только Агент администрирования.
  - Не установлен Агент администрирования и антивирусная защита.

  Количество устройств количество SVM и компьютеров, на которых установлены указанные компоненты и программы.

  В строке ниже в поле Количество устройств отображается общее количество SVM и компьютеров, на которых установлены компоненты защиты "Лаборатории Касперского".

Отчет содержит следующую детальную информацию:

- Группа – название группы администрирования, в которую входит SVM с установленным компонентом Kaspersky Security, или название группы администрирования, в которую входит компьютер с установленными Агентом администрирования Kaspersky Security Center.
- Устройство – имя SVM с установленным компонентом Kaspersky Security или имя компьютера, на котором установлен Агент администрирования Kaspersky Security Center.
- Версия Агента администрирования – версия Агента администрирования Kaspersky Security Center, установленного на клиентском устройстве.
- Название программы безопасности – название установленной программы, обеспечивающей антивирусную защиту. В случае программы Kaspersky Security в поле указывается Kaspersky Kaspersky Security для виртуальных и облачных сред.
- Версия программы безопасности – версия установленной программы, обеспечивающей антивирусную защиту.

Отчет о наиболее заражаемых устройствах

Отчет о наиболее заражаемых устройствах содержит информацию о защищенных виртуальных машинах, в ходе проверки которых обнаружено наибольшее количество зараженных файлов.

В поле Период отображается период времени, данные за который включены в отчет. По умолчанию отчет содержит данные за последние 30 дней, включая дату создания отчета.

Отчет содержит следующую сводную информацию:

- Устройство – имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.
- Опасных объектов – общее количество объектов, обнаруженных на защищенной виртуальной машине за отчетный период.
- Различных объектов – количество различных объектов, которые обнаружены на защищенной виртуальной машине за отчетный период.
- Первая заблокированная попытка запуска – дата и время первого обнаружения объекта на защищенной виртуальной машине.
- Последняя заблокированная попытка запуска – дата и время последнего обнаружения объекта на защищенной виртуальной машине.
- Последнее появление в сети – дата и время последнего события, связанного с защищенной виртуальной машиной, на которой обнаружен объект.

- –
- IP-адрес – IP-адрес защищенной виртуальной машины, на которой обнаружен объект.

  NetBIOS-имя, DNS-имя имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.

  В строке ниже в поле Опасных устройств указано количество защищенных виртуальных машин, в ходе проверки которых обнаружено наибольшее количество зараженных файлов. В поле Опасных групп всегда отображается 0, так как защищенные виртуальные машины не могут входить в группы администрирования Kaspersky Security Center.

Отчет содержит следующую детальную информацию о каждом факте обнаружения:

- Устройство – имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.
- Обнаруженный объект – имя объекта, обнаруженного на защищенной виртуальной машине.
- Обнаружено в – дата и время обнаружения объекта на защищенной виртуальной машине.
- Путь к файлу – путь к файлу на защищенной виртуальной машине, в котором обнаружен объект.
- Тип объекта – тип обнаруженного объекта.
- Действие – результат действия, которое программа Kaspersky Security выполнила над обнаруженным объектом.
- Программа – название программы, обеспечивающей антивирусную защиту. Для программы Kaspersky Security в поле
- указывается Kaspersky Kaspersky Security для виртуальных и облачных сред или Kaspersky Security для виртуальных сред 6.0 Защита без агента (для клиентов).
- Номер версии – номер версии программы, обеспечивающей антивирусную защиту.
- Последнее появление в сети – дата и время последнего события, связанного с защищенной виртуальной машиной, на которой обнаружен объект.
- IP-адрес – IP-адрес защищенной виртуальной машины, на которой обнаружен объект.
- NetBIOS-имя, DNS-имя – имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.
- Компонент – название компонента, который обнаружил угрозу. Возможные значения: Задача проверки и Защита от файловых угроз.
- Технология обнаружения – технология, с помощью которой была обнаружена угроза. Возможные значения: Экспертный анализ, Автоматический анализ, Облачный анализ.

Отчет об угрозах

Отчет об угрозах содержит информацию о вирусах и других вредоносных программах, обнаруженных на защищенных виртуальных машинах, а также информацию о результатах действий над файлами, в которых были обнаружены угрозы.

В поле Период отображается период времени, данные за который включены в отчет. По умолчанию отчет содержит данные за последние 30 дней, включая дату создания отчета.

- –

Отчет содержит следующую сводную информацию:

Обнаруженный объект имя объекта, обнаруженного на защищенных виртуальных машинах.

- Тип объекта – тип обнаруженного объекта.
- Опасных объектов – общее количество указанных объектов, которые были обнаружены на защищенных виртуальных машинах за отчетный период.
- По заключению KSN – количество объектов, обнаруженных с помощью KSN.
- Различных файлов – количество различных файлов, содержащих обнаруженный объект.
- Опасных устройств – количество защищенных виртуальных машин, на которых были обнаружены указанные объекты.
- Первая заблокированная попытка запуска – дата и время первого обнаружения объекта на защищенных виртуальных машинах.
- Последняя заблокированная попытка запуска – дата и время последнего обнаружения объекта на защищенных виртуальных машинах.

  В строке ниже находится следующая сводная информация:

  - Различных объектов – общее количество различных объектов, обнаруженных на всех защищенных виртуальных машинах за отчетный период.
  - Различных файлов – общее количество файлов, содержащих обнаруженные объекты, на всех защищенных виртуальных машинах.
  - Опасных устройств – общее количество защищенных виртуальных машин, на которых были обнаружены объекты в отчетный период.
  - Опасных групп – общее количество групп администрирования Kaspersky Security Center, в которые входят устройства, на которых были обнаружены объекты. В этом поле всегда отображается 0, так как защищенные виртуальные машины не могут входить в группы администрирования Kaspersky Security Center.

Отчет содержит следующую детальную информацию о каждом факте обнаружения угрозы:

- Устройство – имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.
- Обнаруженный объект – имя объекта, обнаруженного на защищенной виртуальной машине.
- Обнаружено в – дата и время обнаружения объекта на защищенной виртуальной машине.
- Путь к файлу – путь к файлу, содержащему обнаруженный объект, на защищенной виртуальной машине.
- Тип объекта – тип обнаруженного объекта.
- Действие – результат действия, которое программа Kaspersky Security выполнила над обнаруженным объектом.
- Программа – программа, обнаружившая объект.
- Номер версии – номер версии программы, обнаружившей объект.
-

- Последнее появление в сети – дата и время последнего события, связанного с защищенной виртуальной машиной, на которой обнаружен объект.
- IP-адрес – IP-адрес защищенной виртуальной машины, на которой обнаружен объект.
- NetBIOS-имя, DNS-имя – имя защищенной виртуальной машины, на которой обнаружен объект, и путь к ней в виртуальной инфраструктуре.
- Компонент – название компонента, который обнаружил угрозу. Возможные значения: Задача проверки и Защита от файловых угроз.
- Технология обнаружения – технология, с помощью которой была обнаружена угроза. Возможные значения: Экспертный анализ, Автоматический анализ, Облачный анализ.

Отчет об ошибках

Отчет об ошибках содержит информацию об ошибках, возникших в работе программы.

В поле Период отображается период времени, данные за который включены в отчет. По умолчанию отчет содержит данные за последние 30 дней, включая дату создания отчета.

Отчет содержит следующую сводную информацию:

- Тип ошибки – тип ошибки, зафиксированной в работе программы. Например, Задача завершена с ошибкой.
- Количество ошибок – количество зафиксированных ошибок указанного типа.
- Количество программ – количество программ, в работе которых зафиксирована ошибка указанного типа.
- Количество устройств – количество SVM, на которых зафиксирована ошибка указанного типа, или количество защищенных виртуальных машин, в ходе проверки или защиты которых зафиксирована ошибка указанного типа.
- Количество групп – количество групп администрирования, содержащих SVM, на которых зафиксированы ошибки указанного типа. Для ошибок, зафиксированных в ходе проверки или защиты виртуальных машин, указывается 0, так как защищенные виртуальные машины не могут входить в группы администрирования Kaspersky Security Center.
- Впервые обнаружена – дата и время первого обнаружения ошибки.
- Последний раз обнаружена – дата и время последнего обнаружения ошибки.

  В строке ниже находится следующая сводная информация:

  - Общее количество ошибок – общее количество ошибок, зафиксированных за отчетный период.
  - Типов ошибок – общее количество типов ошибок, зафиксированных за отчетный период.
  - Количество устройств – общее количество SVM, на которых были зафиксированы ошибки, и защищенных виртуальных машин, в ходе проверки или защиты которых зафиксированы ошибки.
  - Количество групп – общее количество групп администрирования, содержащих SVM, на которых зафиксированы ошибки. Ошибки, зафиксированные в ходе проверки или защиты виртуальных машин, при подсчете количества групп не

учитываются, так как защищенные виртуальные машины не могут входить в группы администрирования Kaspersky Security Center.

Отчет содержит следующую детальную информацию о каждой ошибке:

- Группа – название группы администрирования, содержащей SVM, на которой зафиксирована ошибка. Для ошибок, зафиксированных в ходе проверки или защиты виртуальных машин, указывается N/A, так как защищенные виртуальные машины не могут входить в группы администрирования Kaspersky Security Center.
- Устройство – имя SVM, на которой зафиксирована ошибка, или имя защищенной виртуальной машины, в ходе проверки или защиты которой зафиксирована ошибка.
- Программа – название программы, в работе которой зафиксирована ошибка.
- Тип ошибки – тип ошибки. Например, Задача завершена с ошибкой.
- Описание ошибки – подробное описание ошибки.
- Обнаружено – дата и время возникновения ошибки.
- Задача – задача, в ходе выполнения которой зафиксирована ошибка. Если ошибка не связана с выполнением задачи, указывается N/A.
- IP-адрес – IP-адрес SVM, на которой зафиксирована ошибка, или IP-адрес защищенной виртуальной машины, в ходе проверки или защиты которой зафиксирована ошибка.
- Последнее появление в сети – дата и время, когда SVM была видна в локальной сети организации последний раз, или дата и время последнего события, связанного с защищенной виртуальной машиной.
- Последнее соединение с Сервером администрирования – дата и время последнего соединения SVM, на которой зафиксирована ошибка, с Сервером администрирования Kaspersky Security Center.
- NetBIOS-имя – имя защищенной виртуальной машины, в ходе проверки или защиты которой зафиксирована ошибка.
- DNS-имя – доменное имя SVM, на которой зафиксирована ошибка, или имя защищенной виртуальной машины, в ходе проверки или защиты которой зафиксирована ошибка, и путь к ней в виртуальной инфраструктуре.

Отчет об используемых базах

Отчет об используемых базах содержит информацию о версиях и состоянии баз программы, используемых на SVM.

Отчет содержит следующую сводную информацию:

- Созданы – дата и время создания баз программы, используемых на SVM.
- Количество записей – количество записей в этих базах.
- Количество устройств – количество SVM, на которых используются эти базы.
- Количество групп – количество групп администрирования, в которые входят SVM с используемыми базами программы.
- Статус антивирусных баз – информация о том, являются ли базы программы, используемые на SVM, актуальными. Базы на SVM, считаются актуальными, если дата их выпуска совпадает с датой выпуска баз в хранилище Сервера администрирования Kaspersky Security Center.

  В строке ниже находится следующая сводная информация:

  - Количество наборов баз – общее количество наборов баз программы, используемых на SVM.
  - Актуальные – количество баз программы, используемых на SVM, со статусом "актуальные".
  - Обновлены в последние 24 часа – общее количество баз, обновленных на SVM в течение последних 24 часов.
  - Обновлены в последние 3 дня – общее количество баз, обновленных на SVM в течение последних трех дней.
  - Обновлены в последние 7 дней – общее количество баз, обновленных на SVM в течение последних семи дней.
  - Обновлены более 7 дней назад – общее количество баз, обновленных на SVM более семи дней назад.

Отчет содержит следующую детальную информацию:

- Группа – название группы администрирования, в которую входят SVM с используемыми базами программы.
- Устройство – имя SVM.
- Программа – название программы, установленной на SVM.
- Номер версии – номер версии программы, установленной на SVM.
- Созданы – дата и время создания баз программы, используемых на SVM.
- Количество записей – количество записей в этих базах.
- IP-адрес – IP-адрес SVM.
- DNS-имя – доменное имя SVM с используемыми базами программы.
- Последнее появление в сети – дата и время, когда SVM была видна в локальной сети организации последний раз.
- Последнее соединение с Сервером администрирования – дата и время последнего соединения SVM с Сервером администрирования Kaspersky Security Center.
- Статус антивирусных баз – информация о том, являются ли базы программы, используемые на SVM, актуальными. Базы на SVM, считаются актуальными, если дата их выпуска совпадает с датой выпуска баз в хранилище Сервера администрирования Kaspersky Security Center.

- Версия Агента администрирования – версия Агента администрирования Kaspersky Security Center, установленного на SVM с используемыми базами программы.

Отчет о сетевых атаках

Отчет о сетевых атаках содержит сведения о зарегистрированных сетевых атаках на защищенные виртуальные машины и об обнаружении подозрительной сетевой активности, которая может быть признаком вторжения в защищаемую инфраструктуру.

Шаблон отчета о сетевых атаках по умолчанию не содержится в списке шаблонов отчетов на закладке Отчеты. Чтобы добавить шаблон отчета о сетевых атаках в список шаблонов, используйте мастер создания шаблона отчета (см. подробнее в документации Kaspersky Security Center). После окончания работы мастера сформированный шаблон отчета будет добавлен в список на закладке Отчеты.

В поле Период отображается период времени, данные за который включены в отчет.

Отчет содержит следующую сводную информацию:

- Атака – тип сетевой атаки или подозрительной сетевой активности.
- Случаев атак – количество зарегистрированных сетевых атак или случаев обнаружения подозрительной сетевой активности этого типа.
- Атакующих адресов – количество IP-адресов, с которых были зарегистрированы сетевые атаки или которые проявляли подозрительную сетевую активность этого типа.
- Атаковано устройств – количество защищенных виртуальных машин, в трафике которых зарегистрирована активность, характерная для сетевых атак, или подозрительная сетевая активность этого типа.
- Атаковано групп – для программы Kaspersky Security в этом поле всегда указывается 1, так как все защищенные виртуальные машины приписаны к одной условной группе "pseudohosts". Группа "pseudohosts" не является группой администрирования и не отображается в Консоли администрирования Kaspersky Security Center. Защищенные виртуальные машины не могут входить в группы администрирования, поскольку не являются клиентскими устройствами Kaspersky Security Center.
- Первая заблокированная попытка запуска – дата и время первого обнаружения активности, характерной для сетевых атак, или подозрительной сетевой активности этого типа.
- Последняя заблокированная попытка запуска – дата и время последнего обнаружения активности, характерной для сетевых атак, или подозрительной сетевой активности этого типа.

  В строке ниже находится следующая сводная информация:

  - Случаев атак – количество зарегистрированных сетевых атак или подозрительной сетевой активности всех типов.
  - Различных атак – количество типов зарегистрированных сетевых атак или подозрительной сетевой активности.
  - Атакующих адресов – общее количество IP-адресов, с которых были зарегистрированы сетевые атаки или которые проявляли подозрительную сетевую активность.

- Атаковано устройств – общее количество защищенных виртуальных машин, в трафике которых зарегистрирована активность, характерная для сетевых атак, или подозрительная сетевая активность.

- Атаковано групп – для программы Kaspersky Security в этом поле всегда указывается 1, так как все защищенные виртуальные машины приписаны к одной условной группе "pseudohosts". Группа "pseudohosts" не является группой администрирования и не отображается в Консоли администрирования Kaspersky Security Center. Защищенные виртуальные машины не могут входить в группы администрирования, поскольку не являются клиентскими устройствами Kaspersky Security Center.

- Первая заблокированная попытка запуска – дата и время первого обнаружения активности, характерной для сетевых атак, или подозрительной сетевой активности любого типа.

- Последняя заблокированная попытка запуска – дата и время последнего обнаружения активности, характерной для сетевых атак, или подозрительной сетевой активности любого типа.

Отчет содержит следующую детальную информацию о каждом случае обнаружения активности, характерной для сетевых атак, или подозрительной сетевой активности:

- Группа – для программы Kaspersky Security в этом поле всегда указывается pseudohosts, так как все защищенные виртуальные машины приписаны к одной условной группе "pseudohosts". Защищенные виртуальные машины не могут входить в группы администрирования, поскольку не являются клиентскими устройствами Kaspersky Security Center.

- Устройство – имя защищенной виртуальной машины, в трафике которой зарегистрирована сетевая атака или подозрительная сетевая активность.

- Атакующий адрес – IP-адрес, с которого была произведена сетевая атака или который проявлял подозрительную сетевую активность.

- Время атаки – дата и время обнаружения сетевой атаки или подозрительной сетевой активности.
- Атака – тип сетевой атаки или подозрительной сетевой активности.
- Протокол – протокол соединения, в котором была зафиксирована сетевая атака или подозрительная сетевая активность.
- Порт – номер порта, через который была произведена сетевая атака или на котором зафиксирована подозрительная сетевая активность.
- Последнее появление в сети – дата и время последнего события, связанного с защищенной виртуальной машиной, в трафике которой зарегистрирована сетевая атака или подозрительная сетевая активность.
- IP-адрес – IP-адрес защищенной виртуальной машины, в трафике которой зарегистрирована сетевая атака или подозрительная сетевая активность.
- NetBIOS-имя, DNS-имя – имя защищенной виртуальной машины, в трафике которой зарегистрирована сетевая атака или подозрительная сетевая активность, и путь к виртуальной машине в виртуальной инфраструктуре.
- Номер версии – номер версии компонента Защита от сетевых угроз Kaspersky Security.
- Адрес атакуемого интерфейса – IP-адрес, на который была произведена сетевая атака.

Отчет о работе Веб-Контроля

Отчет о работе Веб-Контроля содержит сведения об обращениях пользователей или программ, установленных на защищенных виртуальных машинах, к опасным и нежелательным веб-адресам, то есть к веб-адресам, которые относятся к выбранным для обнаружения категориям веб-адресов.

В поле Период отображается период времени, данные за который включены в отчет. По умолчанию отчет содержит данные за последние 30 дней, включая дату создания отчета.

Отчет содержит следующую сводную информацию:

- Результат – результат действия, которое программа Kaspersky Security выполнила при обнаружении попытки обращения к опасному или нежелательному веб-адресу.
- Правило – сетевое правило, в соответствии с которым программа выполняет действие при обнаружении попытки обращения к опасному или нежелательному веб-адресу. Возможные значения для программы Kaspersky Security:
  - Kaspersky Security для виртуальных сред Защита без агента: Обращение к вредоносному веб-адресу;
  - Kaspersky Security для виртуальных сред Защита без агента: Обращение к фишинговому веб-адресу;
  - Kaspersky Security для виртуальных сред Защита без агента: Обращение к рекламному веб-адресу;
  - Kaspersky Security для виртуальных сред Защита без агента: Обращение к веб-адресу из категории "Другие веб-адреса".
- Попыток – количество попыток обращения к опасным или нежелательным веб-адресам.
- Учетных записей – количество защищенных виртуальных машин, с которых произведена попытка обращения к опасному или нежелательному веб-адресу.
- Веб-адрес – количество опасных или нежелательных веб-адресов, к которым была обнаружена попытка обращения.
- Устройств – количество защищенных виртуальных машин, на которых обнаружена попытка обращения к опасному или нежелательному веб-адресу.
- Групп администрирования – для программы Kaspersky Security в этом поле всегда указывается 1, так как все защищенные виртуальные машины приписаны к одной условной группе "pseudohosts". Группа "pseudohosts" не является группой администрирования и не отображается в Консоли администрирования Kaspersky Security Center. Защищенные виртуальные машины не могут входить в группы администрирования, поскольку не являются клиентскими устройствами Kaspersky Security Center.
- Первая попытка – дата и время первой попытки обращения к опасному или нежелательному веб-адресу.
- Последняя попытка – дата и время последней попытки обращения к опасному или нежелательному веб-адресу.

В строке ниже находится следующая сводная информация:

- Правил – количество сетевых правил, в соответствии с которыми программа выполняет действие при обнаружении попытки обращения к опасному или нежелательному веб-адресу. Для программы Kaspersky Security в этом поле указано 4.

- Блокировок – количество обращений к опасным или нежелательным веб-адресам, к которым программа Kaspersky Security заблокировала доступ.
- Предупреждений – количество обращений к опасным или нежелательным веб-адресам, доступ к которым разрешен в соответствии с параметрами программы.
- Заблокированных веб-адресов – количество опасных и нежелательных веб-адресов, к которым программа Kaspersky Security заблокировала доступ.
- Веб-адресов с предупреждением – количество опасныхх и нежелательных веб-адресов, доступ к которым разрешен в соответствии с параметрами программы.
    - Заблокированных пользователей – количество защищенных виртуальных машин, с которых произведена попытка обращения к заблокированным веб-адресам.
    - Предупрежденных пользователей – количество защищенных виртуальных машин, для которых программа Kaspersky Security разрешила доступ к опасным или нежелательным веб-адресам.
    - Первая блокировка – дата и время первой попытки обращения к опасному или нежелательному веб-адресу, к которому программа Kaspersky Security заблокировала доступ.
    - Последняя блокировка – дата и время последней попытки обращения к опасному или нежелательному вебадресу, к которому программа Kaspersky Security заблокировала доступ.
    - Первое предупреждение – дата и время первого обращения к опасному или нежелательному веб-адресу, доступ к которому разрешен в соответствии с параметрами программы.
    - Последнее предупреждение – дата и время последнего обращения к опасному или нежелательному вебадресу, доступ к которому разрешен в соответствии с параметрами программы.

Отчет содержит следующую детальную информацию для каждого обращения к опасному или нежелательному вебадресу:

- Результат – результат действия, которое программа Kaspersky Security выполнила при обнаружении попытки обращения к опасному или нежелательному веб-адресу.
- Правило – сетевое правило, в соответствии с которым программа выполняет действие при обнаружении попытки обращения к опасному или нежелательному веб-адресу. Возможные значения для программы Kaspersky Security:
    - Kaspersky Security для виртуальных сред Защита без агента: Обращение к вредоносному веб-адресу;
    - Kaspersky Security для виртуальных сред Защита без агента: Обращение к фишинговому веб-адресу;
    - Kaspersky Security для виртуальных сред Защита без агента: Обращение к рекламному веб-адресу;
    - Kaspersky Security для виртуальных сред Защита без агента: Обращение к веб-адресу из категории "Другие веб-адреса".
- Учетная запись – IP-адрес защищенной виртуальной машины, с которой произведена попытка обращения к опасному или нежелательному веб-адресу.

- Веб-адрес – опасный или нежелательный веб-адрес, к которому была обнаружена попытка обращения.
- Время – дата и время обнаружения попытки обращения к опасному или нежелательному веб-адресу.
- Группа – для программы Kaspersky Security в этом поле всегда указывается pseudohosts, так как все защищенные виртуальные машины приписаны к одной условной группе "pseudohosts". Группа "pseudohosts" не является группой администрирования и не отображается в Консоли администрирования Kaspersky Security Center. Защищенные виртуальные машины не могут входить в группы администрирования, поскольку не являются клиентскими устройствами Kaspersky Security Center.
- Устройство – имя защищенной виртуальной машины, на которой обнаружена попытка обращения к опасному или нежелательному веб-адресу, и путь к виртуальной машине в виртуальной инфраструктуре.
- Номер версии – номер версии компонента Защита от сетевых угроз Kaspersky Security, обнаружившего попытку обращения к опасному или нежелательному веб-адресу.
- Последнее появление в сети – дата и время последнего события, связанного с защищенной виртуальной машиной, на которой обнаружена попытка обращения к опасному или нежелательному веб-адресу.
- IP-адрес – IP-адрес защищенной виртуальной машины, на которой обнаружена попытка обращения к опасному или нежелательному веб-адресу.
- NetBIOS-имя, DNS-имя – имя защищенной виртуальной машины, на которой обнаружена попытка обращения к опасному или нежелательному веб-адресу, и путь к виртуальной машине в виртуальной инфраструктуре.
- По заключению KSN – информация о том, была ли попытка обращения к опасному или нежелательному вебадресу обнаружена с помощью KSN. Возможные значения: Да или Нет.

Отчет о состоянии защиты

Отчет о состоянии защиты содержит сведения о состоянии программы защиты (Kaspersky Security), установленной на клиентских устройствах Kaspersky Security Center (SVM), и сведения о состоянии защиты виртуальных машин.

С помощью отчета о состоянии защиты вы можете получить сведения о проблемах в защите виртуальной инфраструктуры. По умолчанию в отчете отображаются устройства со статусами Критический и Предупреждение. Если требуется, в окне свойства отчета в разделе Параметры вы можете настроить включение в отчет информации об устройствах со статусом ОК.

Отчет содержит следующую сводную информацию:

- Статус – статус клиентского устройства (SVM) или статус защиты виртуальной машины.
- Причина добавления в отчет – причина или причины присвоения текущего статуса.
- Количество незащищенных устройств – количество SVM и виртуальных машин, которые имеют указанную причину присвоения статуса.

- Количество групп – для SVM с указанной причиной присвоения статуса клиентского устройства указывается количество групп администрирования, в которые входят SVM. Для виртуальных машин с указанной причиной присвоения статуса защиты указывается количество групп администрирования, в которые входят SVM, защищающие эти виртуальные машины.

  В строке ниже в поле Количество незащищенных устройств указано общее количество SVM и виртуальных машин, добавленных в отчет. В поле Количество групп указано общее количество групп администрирования, в которые входят SVM, добавленные в отчет, и SVM, защищающие виртуальные машины, добавленные в отчет.

Отчет содержит следующую детальную информацию об SVM и о виртуальных машинах, добавленных в отчет:

- Статус – статус клиентского устройства (SVM) или статус защиты виртуальной машины.
- Группа – для SVM, добавленной в отчет, указывается название группы администрирования, в которую входит SVM. Для виртуальной машины, добавленной в отчет, указывается название группы администрирования, в которую входит SVM, защищающая эту виртуальную машину.
- Устройство – имя SVM или виртуальной машины.
- Последнее соединение с Сервером администрирования – для SVM, добавленной в отчет, указывается дата и время последнего соединения SVM с Сервером администрирования Kaspersky Security Center. Для виртуальной машины, добавленной в отчет, указывается N/A.
- Причина добавления в отчет – причина присвоения текущего статуса клиентского устройства SVM или статуса защиты виртуальной машине.
- Статус устройства определен программой – причина присвоения статуса, если Kaspersky Security Center получил статус устройства от управляемой программы, то есть от Kaspersky Security.
- IP-адрес – IP-адрес SVM или виртуальной машины. Если определить IP-адрес не удалось (например, когда виртуальная машина выключена), в отчете отображается 0.0.0.0.
- Последнее появление в сети – дата и время последнего соединения SVM с Сервером администрирования Kaspersky Security Center или дата и время последнего события, связанного с виртуальной машиной.
- NetBIOS-имя – имя виртуальной машины и путь к ней в виртуальной инфраструктуре.
- DNS-имя – доменное имя SVM или имя виртуальной машины и путь к ней в виртуальной инфраструктуре.
- Операционная система – операционная система, установленная на SVM или на виртуальной машине.
- Дата выпуска антивирусной базы – для SVM, добавленной в отчет, указывается дата и время выпуска баз программы, установленных на SVM в текущий момент. Для виртуальной машины, добавленной в отчет, указывается дата и время выпуска баз программы, установленных на SVM, которая защищает эту виртуальную машину.
- Последняя полная проверка – дата и время завершения последней задачи полной проверки.

Просмотр отчетов

Чтобы просмотреть отчет, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите узел Сервер администрирования.

. В рабочей области узла перейдите на закладку Отчеты и выберите шаблон отчета, который вы хотите просмотреть.

В рабочей области отобразится отчет, сформированный по выбранному шаблону.

Шаблон отчета о сетевых атаках по умолчанию не содержится в списке шаблонов отчетов на закладке Отчеты. Чтобы добавить шаблон отчета о сетевых атаках в список шаблонов, используйте мастер создания шаблона отчета (см. подробнее в документации Kaspersky Security Center). После окончания работы мастера сформированный шаблон отчета будет добавлен в список на закладке Отчеты.

В отчете отображаются следующие сведения:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы создан отчет; графическая диаграмма, отображающая наиболее характерные данные отчета; сводная таблица с вычисляемыми
- показателями отчета; таблица с детальными данными отчета.
-
- Более подробную информацию о работе с отчетами см. в документации Kaspersky Security Center.

Просмотр статистики работы программы

Вы можете посмотреть статистику работы Kaspersky Security на каждой SVM в Консоли администрирования Kaspersky Security Center.

Чтобы просмотреть статистику работы программы на SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте окно свойств SVM:

a. Выберите группу администрирования, содержащую кластер KSC, в котором находится нужная SVM. b. В рабочей области выберите закладку Устройства.

c. В списке выберите SVM и откройте окно свойств SVM двойным щелчком мыши или выбрав пункт Свойства в контекстном меню.

Откроется окно Свойства: <Имя SVM>.

. В окне свойств SVM в списке слева выберите раздел Программы.

В правой части окна отобразится список программ, установленных на этой SVM.

. Выберите программу Kaspersky Kaspersky Security для виртуальных и облачных сред и нажмите на кнопку Статистика, расположенную под списком программ.

Откроется окно Статистика.

Если вы выбрали SVM с компонентом Защита от файловых угроз, в окне Статистика отображается следующая информация:

- Информация о базах программы – дата и время выпуска баз программы, а также количество записей в базах или информация о том, что базы программы повреждены.

  Эта информация отображается, только если базы программы установлены.

- Информация о версии – версия библиотеки EPSEC, установленной на SVM.

- Информация о лицензии – количество дней, оставшееся до окончания срока действия лицензии, или информация о том, что срок действия лицензии истек или лицензионный ключ заблокирован. Если вы используете программу по неограниченной подписке, отображается не установлен.

- Общая статистика – количество объектов, проверенных на SVM с момента установки программы во время защиты виртуальных машин и при выполнении задач проверки.

- Самые проверяемые файлы – 20 наиболее часто проверяемых файлов за последние 24 часа.

- Статистика за последние 24 часа – количество объектов, проверенных на SVM за последние 24 часа во время защиты виртуальных машин и при выполнении задач проверки.

- Статистика за последние 30 дней – количество объектов, проверенных на SVM за последние 30 дней во время защиты виртуальных машин и при выполнении задач проверки.

- Статистика за последние 7 дней – количество объектов, проверенных на SVM за последние семь дней во время защиты виртуальных машин и при выполнении задач проверки.

Если вы выбрали SVM с компонентом Защита от сетевых угроз, в окне Статистика отображается следующая информация:

- Информация о базах программы – дата и время выпуска баз программы, а также количество записей в базах или информация о том, что базы программы повреждены.

  Эта информация отображается, только если базы программы установлены.

- Информация о лицензии – количество дней, оставшееся до окончания срока действия лицензии, или информация о том, что срок действия лицензии истек или лицензионный ключ заблокирован. Если вы используете программу по неограниченной подписке, отображается не установлен.

- Общая статистика – количество сетевых пакетов, обработанных на SVM с момента установки программы во время защиты виртуальных машин.

- Статистика за последние 24 часа – количество сетевых пакетов, обработанных на SVM за последние 24 часа.

- Статистика за последние 30 дней – количество сетевых пакетов, обработанных на SVM за последние 30 дней.

- Статистика за последние 7 дней – количество сетевых пакетов, обработанных на SVM за последние семь дней.

Обновление информации в окне Статистика выполняется при открытии окна или по кнопке Обновить, расположенной в верхней части окна. Обновление информации в реальном времени не выполняется.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальных машин, Kaspersky Security может использовать данные, полученные от пользователей программ "Лаборатории Касперского" во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

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

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

В зависимости от расположения инфраструктуры KSN различают:

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

Информация о том, какой тип KSN использует программа Kaspersky Security, отображается в свойствах политики.

Взаимодействие между SVM, находящимися под управлением Kaspersky Security Center, и инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Для использования KSN в работе Kaspersky Security служба проксисервера KSN должна быть включена в Kaspersky Security Center.
Для использования Локального KSN требуется включить и настроить использование Локального KSN в Kaspersky Security Center.

Настройка службы прокси-сервера KSN и Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе Прокси-сервер KSN. См. подробнее в документации Kaspersky Security Center. Настройка использования KSN в работе программы Kaspersky Security выполняется в свойствах политики.

> Если служба прокси-сервера KSN выключена в Kaspersky Security Center, обмен данными между SVM и KSN не производится. Если при этом использование KSN включено в политике Kaspersky Security, возможно снижение производительности работы программы. Рекомендуется выключить использование KSN в политике Kaspersky Security, если служба прокси-сервера KSN выключена в Kaspersky Security Center.

Kaspersky Security автоматически отправляет в "Лабораторию Касперского" информацию об использовании KSN, а также может отправлять другую информацию в зависимости от выбранного вами режима использования KSN (стандартный KSN или расширенный KSN). Режим KSN влияет на объем данных, которые передаются в "Лабораторию Касперского" при использовании KSN.

Ваше участие в Kaspersky Security Network при использовании расширенного KSN позволяет “Лаборатории Касперского” оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации.

Участие в Kaspersky Security Network является добровольным. Решение об участии в Kaspersky Security Network принимается при создании политики, его можно изменить в любой момент.

О предоставлении данных при использовании Kaspersky Security Network

Если вы участвуете в Kaspersky Security Network и используете KSN в стандартном режиме, вы соглашаетесь передавать в "Лабораторию Касперского" в автоматическом режиме следующие данные:

- Информацию, необходимую для проверки файлов: имя и идентификатор обнаруженной угрозы согласно классификации "Лаборатории Касперского", хеш проверяемого объекта и тип хеш-функции, идентификатор используемых антивирусных баз.
- Информацию о проверяемых веб-адресах: веб-адрес или IP-адрес, по которому запрашивается репутация, вебадрес страницы, с которой осуществлен переход на проверяемый веб-адрес, идентификатор протокола соединения и номер используемого порта.
- Информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности: хеш (SHA256) сертификата, которым подписан проверяемый объект, и открытый ключ сертификата.
- Общую информацию: тип и полную версию программы Kaspersky Security, информацию о компонентах программы и об обновлении модулей программы, информацию об операционной системе, установленной на SVM и защищенных виртуальных машинах.

Если вы участвуете в Kaspersky Security Network и используете KSN в расширенном режиме, вы соглашаетесь передавать в "Лабораторию Касперского" в автоматическом режиме все данные, перечисленные в Положении о Kaspersky Security Network. В том числе в "Лабораторию Касперского" для проверки 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. Расширенный KSN используется по умолчанию. Вы можете выключить использование расширенного KSN в свойствах политики.

Текст Положения о Kaspersky Security Network вы можете посмотреть в свойствах политики в разделе Параметры KSN.

Информацию о хранении, защите и уничтожении статистической информации, полученной во время использования KSN и переданной в "Лабораторию Касперского", вы можете получить, ознакомившись с Политикой конфиденциальности на веб-сайте "Лаборатории Касперского".

Если вы не участвуете в программе Kaspersky Security Network, то данные, перечисленные в Положении о Kaspersky Security Network, не передаются в "Лабораторию Касперского".

Просмотр Положения о Kaspersky Security Network

Чтобы ознакомиться с Положением о Kaspersky Security Network, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В

рабочей области выберите закладку Политики.

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

. В списке слева выберите раздел Параметры KSN.

. Откройте по ссылке Положение о Kaspersky Security Network.

Текст Положения о Kaspersky Security Network откроется в отдельном окне.

Настройка использования Kaspersky Security Network

Настройка использования KSN в работе программы Kaspersky Security выполняется в параметрах политики. Если в активной политике 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 KSN в работе Kaspersky Security, убедитесь в том, что использование KSN нужного вам типа настроено в Kaspersky Security Center. Для использования Глобального KSN в Kaspersky Security Center должна быть включена служба прокси-сервера KSN. Для использования Локального KSN требуется включить и настроить использование Локального KSN в Kaspersky Security Center. Настройка службы прокси-сервера KSN и Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе Прокси-сервер KSN. См. подробнее в документации Kaspersky Security Center.

Чтобы настроить использование KSN в работе программы Kaspersky Security, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, в области действия которой находятся нужные виртуальные машины:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей

области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Параметры KSN.

. Если вы хотите использовать Глобальный KSN в работе программы, выполните следующие действия: a.

Установите флажок Использовать KSN.

b. В открывшемся окне ознакомьтесь с Положением о Kaspersky Security Network.

c. Если вы согласны со всеми пунктами Положения, выберите вариант Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network и нажмите на кнопку ОК.

d. По умолчанию Глобальный KSN используется в расширенном режиме. Режим KSN влияет на объем данных, которые автоматически передаются в "Лабораторию Касперского" при использовании KSN. Если вы хотите выключить использование расширенного KSN, снимите флажок Использовать расширенный KSN.

. Если вы хотите выключить использование Глобального KSN, снимите флажок Использовать KSN.

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

. Если вы хотите выключить использование Локального KSN, снимите флажок Использовать Локальный KSN.

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

SNMP-мониторинг состояния SVM

Вы можете получать информацию о состоянии SVM, развернутых в виртуальной инфраструктуре, с помощью любой системы сетевого управления, использующей протокол SNMP. На SVM установлен агент SNMP, который может передавать информацию о состоянии SVM системе сетевого управления вашей организации.

Агент SNMP может передавать следующие сведения о состоянии SVM с компонентом Защита от файловых угроз:

- Информацию об использовании оперативной памяти процессом ksvmain в процентах (относительно максимального значения, при достижении которого программа перезапускается).

- Количество защищенных виртуальных машин с операционными системами для рабочих станций и количество защищенных виртуальных машин с операционными системами для серверов.

  При подсчете количества защищенных виртуальных машин учитываются все виртуальные машины, которые находились под защитой программы за последние 30 дней, даже если в текущий момент эти виртуальные машины выключены.

- Информацию о том, выполняются ли на SVM в текущий момент задачи проверки виртуальных машин.

- Если задачи проверки выполняются, информацию о количестве виртуальных машин, которые ожидают проверки в текущий момент времени, и о количестве одновременно проверяемых виртуальных машин.

- Информацию о состоянии служб компонента Защита от файловых угроз на SVM: On (службы запущены) или Off (службы не запущены).

Для SVM с компонентом Защита от сетевых угроз агент SNMP может передавать информацию об использовании оперативной памяти процессом nsmain в процентах (относительно максимального значения, при достижении которого программа перезапускается).

Эти данные специфичны для программы, информация о них содержится в MIB-файлах KSV-MIB.txt и KSVNSMIB.txt, которые поставляются вместе с программой. Вы можете использовать эти файлы для получения дополнительной информации от SVM. Вы можете также использовать другие MIB-файлы для получения необходимой информации от SVM.

Вы можете ограничить список IP-адресов, на которые агент SNMP передает информацию о состоянии SVM, чтобы предотвратить несанкционированный доступ к службе SNMP.

Включение и выключение SNMP-мониторинга

Включение и выключение SNMP-мониторинга выполняется в параметрах политики. Если в активной политике, которая определяет параметры работы SVM, SNMP-мониторинг включен, агент SNMP, установленный на SVM, передает информацию о состоянии SVM системе SNMP-мониторинга вашей организации.

Если политика, в которой включен SNMP-мониторинг, не активна, информация о состоянии SVM не передается.

Чтобы включить или выключить SNMP-мониторинг, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Параметры SNMP-мониторинга.

. Выполните одно из следующих действий:

- Установите флажок Включить SNMP-мониторинг состояния SVM, если вы хотите получать информацию о состоянии SVM.
- Снимите флажок Включить SNMP-мониторинг состояния SVM, если вы хотите выключить мониторинг состояния SVM.

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

Ограничение списка получателей информации о состоянии SVM

Вы можете ограничить список IP-адресов, на которые агент SNMP передает информацию о состоянии SVM, чтобы предотвратить несанкционированный доступ к службе SNMP.

Чтобы сформировать список IP-адресов, на которые передается информация о состоянии SVM, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры работы SVM:

a. В дереве консоли выберите папку или группу администрирования, в которой создана политика. b. В рабочей

области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Параметры SNMP-мониторинга.

. Установите флажок Включить SNMP-мониторинг состояния SVM, если SNMP-мониторинг выключен.

. Установите флажок Передавать информацию только на указанные IP-адреса.

. Нажмите на кнопку Добавить или на клавишу **INSERT** и введите в строке списка IP-адрес в формате IPv4 или IPподсеть в следующем формате: <IP-адрес в формате IPv4>/<количество единичных разрядов в маске подсети>.

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

Автоматическая установка патчей программы

Kaspersky Security Center позволяет автоматически загружать и устанавливать патчи программы Kaspersky Security на SVM.

Патчи автоматически загружаются из хранилища Сервера администрирования Kaspersky Security Center во время загрузки пакета обновлений баз программы.

Для установки патчей используется задача автоматической установки патчей.
В результате выполнения задачи патчи устанавливаются на те SVM, на которых эти патчи еще не установлены. При этом выполняется проверка работоспособности программы Kaspersky Security на каждой SVM. Если проверка закончилась неудачно, автоматически выполняется откат установки патчей.

Во время установки патчей защита виртуальных машин и выполнение задач проверки приостанавливаются.

После установки патча на SVM новый номер версии SVM отображается в отчетах и событиях Kaspersky Security Center.

Если после установки патча в работе программы возникают ошибки, вы можете вручную откатить установку патча на SVM. Для получения подробной информации обращайтесь к специалистам Службы технической поддержки.

Настройка автоматической загрузки и установки патчей

Чтобы настроить автоматическую загрузку и установку патчей, выполните следующие действия:

. 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).

. Убедитесь, что в Kaspersky Security Center создана задача обновления баз программы. Если задача обновления отсутствует, создайте ее.

. Создайте задачу автоматической установки патчей. Вы можете создать задачу для всех SVM, для SVM одного кластера KSC или для отдельной SVM.

Создание задачи автоматической установки патчей

Чтобы создать задачу автоматической установки патчей, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку или группу администрирования, в которой вы хотите создать задачу.

Если вы выбрали папку Управляемые устройства или группу администрирования, содержащую кластер KSC, в рабочей области выберите закладку Задачи.

. Нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите тип задачи: Kaspersky Kaspersky Security для виртуальных и облачных сред → Автоматическая установка патчей.

Перейдите к следующему шагу мастера создания задачи.

. Если вы запустили мастер создания задачи из папки Задачи, укажите способ выбора SVM, на которых должна выполняться задача:

- Нажмите на кнопку Выбрать устройства, обнаруженные в сети Сервером администрирования, если вы хотите выбрать SVM из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.

- Нажмите на кнопку Задать адреса устройств вручную или импортировать из списка, если вы хотите задать адреса SVM вручную или импортировать список SVM из файла. Для импорта используется файл формата TXT с перечнем адресов SVM, где каждый адрес должен располагаться в отдельной строке.

> Если вы импортируете список адресов из файла или задаете адреса вручную, а SVM идентифицируются по имени, то в список SVM, для которых создается задача, вы можете добавить только те SVM, информация о которых уже занесена в базу данных Сервера администрирования при подключении SVM или в результате опроса локальной сети организации.

- Нажмите на кнопку Назначить задачу выборке устройств, если задача должна выполняться на всех SVM, входящих в выборку по предопределенному критерию. О создании выборки устройств см. в документации Kaspersky Security Center.

- Нажмите на кнопку Назначить задачу группе администрирования, если задача должна выполняться на всех SVM, входящих в группу администрирования.

  В зависимости от указанного вами способа выбора SVM в открывшемся окне выполните одно из следующих действий:

  - В списке обнаруженных устройств укажите SVM, на которых будет выполняться задача. Для этого установите флажок в списке слева от имени SVM.

- Нажмите на кнопку Добавить или Добавить IP-диапазон и задайте адреса SVM.
- Нажмите на кнопку Импортировать и в открывшемся окне выберите файл формата TXT, содержащий список адресов SVM.
- Нажмите на кнопку Обзор и в открывшемся окне укажите название выборки, содержащей SVM, на которых будет выполняться задача.
- Нажмите на кнопку Обзор и выберите группу администрирования или введите название группы администрирования вручную.

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры расписания 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.

- Использовать случайную задержку запуска задачи в интервале (мин). Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок Использовать автоматическое определение случайного интервала между запусками задачи.

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

Перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи автоматической установки патчей и перейдите к следующему шагу мастера 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 отката обновления отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска задачи, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить или остановить задачу вручную.

Проверка целостности компонентов программы

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

Проверка целостности выполняется для следующих компонентов:

- Плагины управления Kaspersky Security.
- Сервер интеграции.
- Консоль Сервера интеграции.
- SVM.

Проверка целостности компонентов программы выполняется с помощью утилиты проверки целостности integrity_check_tool, расположенной на сертифицированном компакт-диске. Утилита проверяет целостность файлов, перечисленных в специальных списках, которые называются файлы манифеста. Файл манифеста компонента программы содержит файлы, целостность которых важна для корректной работы компонента программы. Целостность самих файлов манифеста также проверяется.

Для запуска утилиты проверки целостности на SVM требуется учетная запись root. Для запуска утилиты проверки целостности остальных компонентов программы требуется учетная запись администратора.

Рекомендуется запускать утилиту проверки целостности с сертифицированного компакт-диска, чтобы гарантировать целостность утилиты. При запуске с компакт-диска требуется указать полный путь к файлу манифеста в папке программы.

Файлы манифеста для компонентов программы расположены по следующим путям:

- для плагинов управления Kaspersky Security – по умолчанию в папках, где расположены исполняемые модули (DLL) плагинов управления:
  - для 64-разрядных операционных систем:
    - C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV5.plg\integrity_check.xml – для основного плагина управления Kaspersky Security;
    - C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\Plugins\KSVT5.plg\integrity_check.xml – для плагина управления Kaspersky Security для клиентов;
  - для 32-разрядных операционных систем:
    - C:\Program Files\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV5.plg\integrity_check.xml – для основного плагина управления Kaspersky Security;
    - C:\Program Files\Kaspersky Lab\Kaspersky Security Center\Plugins\KSVT5.plg\integrity_check.xml – для плагина управления Kaspersky Security для клиентов;
- для Сервера интеграции – по умолчанию в папке, где расположен исполняемый файл Сервера интеграции:
  - C:\Program Files (x86)\Kaspersky Lab\Kaspersky VIIS\integrity_check.xml – для 64-разрядных операционных систем;
  - C:\Program Files\Kaspersky Lab\Kaspersky VIIS\integrity_check.xml – для 32-разрядных операционных систем;
- для Консоли Сервера интеграции – по умолчанию в папке, где расположен исполняемый файл Консоли Сервера интеграции:
  - C:\Program Files (x86)\Kaspersky Lab\Kaspersky VIIS Console\integrity_check.xml – для 64-разрядных операционных систем;
  - C:\Program Files\Kaspersky Lab\Kaspersky VIIS Console\integrity_check.xml – для 32-разрядных операционных систем;
- для SVM:
  - /var/opt/kaspersky/ksv/product/integrity_check.xml – для SVM с установленным компонентом Защита от файловых угроз;
  - /var/opt/kaspersky/ksvns/product/integrity_check.xml – для SVM с установленным компонентом Защита от сетевых угроз;

Чтобы проверить целостность компонента программы, выполните следующую команду: `integrity_check_tool - v [| --verify] -m [| --manifest] <путь к файлу манифеста>`

где `<путь к файлу манифеста>` – полный путь к файлу манифеста.

Вы можете запустить утилиту со следующими необязательными параметрам:

- `-h, --help` – вывод справки о параметрах утилиты.

- `-V, --verbose` – расширенный вывод выполняемых действий и результатов. Если вы не укажете этот параметр, будут выводиться только ошибки, объекты, не прошедшие проверку, и суммарная статистика проверки.

- `-L, --log-file <файл>`, где `<файл>` – имя файла для вывода событий, произошедших во время проверки. По умолчанию события выводится в стандартный поток stdout.

- `-l, --log-level <0-1000>`, где `<0-1000>` – уровень детализации вывода событий. По умолчанию используется уровень детализации `0`.

Результат проверки каждого файла манифеста выводится рядом с названием файла манифеста в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`).

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

Инструкция по работе с программой для администратора организации-клиента

Этот раздел адресован администратору виртуальной инфраструктуры, которая принадлежит организации-клиенту и находится под защитой программы Kaspersky Security, установленной в инфраструктуре организации-провайдера антивирусной защиты.

Этот раздел содержит сведения, необходимые администратору клиента для управления защитой своей виртуальной инфраструктуры.

Для работы с программой Kaspersky Security требуется опыт работы с виртуальной инфраструктурой на платформе VMware vSphere и системой удаленного централизованного управления программами "Лаборатории Касперского" – Kaspersky Security Center.

О Kaspersky Kaspersky Security для виртуальных и облачных сред

Kaspersky Kaspersky Security для виртуальных и облачных сред (далее также "Kaspersky Security") представляет собой интегрированное решение, обеспечивающее защиту виртуальных машин на гипервизоре VMware ESXi от вирусов и других вредоносных программ, а также от сетевых угроз.

Kaspersky Security позволяет защищать виртуальные машины с гостевыми операционными системами Windows, в том числе и с операционными системами для серверов, а также виртуальные машины с гостевыми операционными системами Linux.

В состав Kaspersky Security входят следующие компоненты:

- Защита от файловых угроз. Компонент позволяет избежать заражения объектов файловой системы виртуальной машины. Компонент запускается при старте Kaspersky Security и выполняет функции защиты виртуальных машин и проверки объектов файловой системы виртуальных машин.

- Защита от сетевых угроз. Компонент позволяет обнаруживать и блокировать активность, характерную для сетевых атак, и другую подозрительную сетевую активность, а также проверять веб-адреса, к которым обращается пользователь или какая-либо программа, и блокировать доступ к веб-адресам в случае обнаружения угрозы.

- Сервер интеграции. Компонент осуществляет взаимодействие между компонентами программы Kaspersky Security и виртуальной инфраструктурой VMware.

Компоненты Защита от файловых угроз и Защита от сетевых угроз установлены на SVM, которые развернуты на гипервизорах VMware ESXi в инфраструктуре провайдера антивирусной защиты.

Kaspersky Security предоставляет следующие возможности:

- Защита. Kaspersky Security проверяет все файлы, которые пользователь или какая-либо программа открывает, сохраняет или запускает на виртуальной машине.

  - Если в файле не обнаружены вредоносные программы, программа Kaspersky Security разрешает доступ к этому файлу.

  - Если в файле обнаружены вредоносные программы, программа Kaspersky Security выполняет то действие, которое указано в ее параметрах, например удаляет файл или блокирует доступ к файлу.

  Kaspersky Security может защищать только включенные виртуальные машины.

- Проверка. Программа позволяет выполнять антивирусную проверку файлов виртуальных машин. Требуется периодически проверять файлы виртуальной машины с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов. Вы можете выполнять проверку по требованию или задать расписание проверки.

  Kaspersky Security может проверять включенные виртуальные машины, шаблоны виртуальных машин, а также выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS.

- Предотвращение вторжений. Kaspersky Security позволяет анализировать сетевой трафик защищенных виртуальных машин и обнаруживать сетевые атаки и подозрительную сетевую активность, которая может быть признаком вторжения в защищаемую инфраструктуру. Обнаружив попытку сетевой атаки на виртуальную машину или подозрительную сетевую активность, Kaspersky Security может прерывать соединение и блокировать трафик с IP-адреса, который является источником сетевой атаки или подозрительной сетевой активности.

  Параметры предотвращения вторжений задает провайдер антивирусной защиты.

- Проверка веб-адресов. Kaspersky Security позволяет проверять веб-адреса, к которым пользователь или программа, установленная на виртуальной машине, обращается по протоколу HTTP. Если Kaspersky Security устанавливает принадлежность веб-адреса к одной из категорий веб-адресов, выбранных для обнаружения, программа может блокировать доступ к этому веб-адресу. По умолчанию Kaspersky Security проверяет вебадреса на принадлежность к вредоносным и фишинговым веб-адресам.

  Параметры проверки веб-адресов задает провайдер антивирусной защиты.

- Хранение резервных копий файлов. Программа позволяет хранить резервные копии тех файлов, которые были удалены или изменены в процессе лечения. Если вылеченный файл содержал информацию, которая в результате лечения стала полностью или частично недоступна, файл может быть сохранен из его резервной копии.

  Все действия с резервными копиями файлов выполняет провайдер антивирусной защиты.

Об управлении программой

Управление Kaspersky Security осуществляется через систему удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

Интерфейс для управления программой Kaspersky Security через Kaspersky Security Center обеспечивает плагин управления Kaspersky Security для клиентов. Плагин управления должен быть установлен на том компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.

Управление работой программы Kaspersky Security осуществляется с помощью политик и задач.

Политика – это набор параметров, с которыми SVM защищают виртуальные машины, входящие в состав защищаемой инфраструктуры. Каждая политика содержит один или несколько профилей защиты. Профили защиты позволяют настроить параметры файловой защиты виртуальных машин.

Задачи запускаются на SVM и позволяют выполнять проверку виртуальных машин.

Kaspersky Security отправляет на Сервер администрирования Kaspersky Security Center информацию обо всех событиях, произошедших во время антивирусной защиты и проверки виртуальных машин, а также о событиях, произошедших во время защиты от вторжений и проверки веб-адресов. Вы можете получать уведомления о событиях и просматривать их в Kaspersky Security Center.

Подробную информацию о работе с событиями, политиками и задачами см. в документации Kaspersky Security Center.

О политиках Kaspersky Security

Политика позволяет настраивать параметры файловой защиты виртуальных машин с помощью профилей защиты, а также параметры использования Kaspersky Security Network.

Политики создаются с помощью мастера, который запускается по кнопке Новая политика, расположенной в рабочей области папки Управляемые устройства на закладке Политики.

Вы можете создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

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

Чтобы открыть окно свойств политики, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства.

. В рабочей области выберите закладку Политики.

. В списке политик выберите политику и откройте окно Свойства: <Название политики> двойным щелчком мыши по политике или выбрав в контекстном меню пункт Свойства.

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

О профилях защиты

В политиках Kaspersky Security предусмотрены следующие профили защиты:

- Основной профиль защиты автоматически формируется во время создания политики. Основной профиль защиты недоступен для удаления, однако вы можете изменять значения параметров основного профиля защиты.

- Дополнительные профили защиты вы можете создать после создания политики. Благодаря дополнительным профилям защиты вы можете гибко настраивать разные параметры защиты для разных виртуальных машин в составе защищаемой инфраструктуры. Политика может содержать несколько дополнительных профилей защиты.

В профилях защиты вы можете настраивать следующие параметры:

- Уровень безопасности. Вы можете выбрать один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий) или настроить уровень безопасности самостоятельно (Пользовательский). Уровень безопасности определяет следующие параметры проверки:

  - проверка архивов, самораспаковывающихся архивов, вложенных OLE-объектов, составных файлов;

  - ограничение проверки файлов по времени; список объектов для обнаружения.

  - Действие, которое выполняет Kaspersky Security, если обнаруживает зараженные файлы.

- Область защиты (проверка сетевых дисков во время защиты виртуальных машин).

- Исключения из защиты (по имени, расширению или пути к файлу, по маске файла или по пути к папке, файлы которой не надо проверять).

Профиль защиты может быть назначен отдельному объекту виртуальной инфраструктуры VMware или корневому элементу защищаемой инфраструктуры, в роли которого выступает условный объект "Организация vCloud Director". Профиль защиты, назначенный корневому элементу защищаемой инфраструктуры, по умолчанию наследуется всеми дочерними элементами защищаемой инфраструктуры (виртуальными машинами и их объединениями).

Профили защиты наследуются также согласно иерархии объектов виртуальной инфраструктуры VMware: профиль защиты, назначенный объекту виртуальной инфраструктуры, наследуется всеми его дочерними объектами, в том числе и виртуальными машинами, если дочернему объекту / виртуальной машине не назначен собственный профиль защиты или если дочерний объект / виртуальная машина не исключены из защиты. Таким образом, вы можете назначить виртуальной машине собственный профиль защиты или использовать для нее профиль защиты, унаследованный от родительского объекта.

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

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

Если вы исключаете объект виртуальной инфраструктуры из защиты, то все дочерние объекты, у которых профиль защиты унаследован от родительского объекта, тоже исключаются из защиты. Вы можете исключить из защиты все дочерние объекты, которым назначен собственный профиль защиты, или оставить их под защитой программы.

Наследование профилей защиты позволяет назначать одинаковые параметры защиты нескольким виртуальным машинам одновременно. Например, вы можете назначить одинаковые профили защиты всем виртуальным машинам в составе виртуального Datacenter.

О задачах

Для Kaspersky Security предусмотрены следующие задачи:

- Задача полной проверки виртуальных машин. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин в вашей виртуальной инфраструктуре.

- Задача выборочной проверки виртуальных машин. Задача позволяет выполнять антивирусную проверку файлов тех виртуальных машин, которые вы указали в параметрах задачи. Вы можете указывать отдельные виртуальные машины или объекты виртуальной инфраструктуры VMware более высокого уровня иерархии.

Задачи создаются с помощью мастера, который запускается по кнопке Новая задача, расположенной в рабочей области папки Управляемые устройства на закладке Задачи.

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

Чтобы открыть окно свойств задачи, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства.

. В рабочей области выберите закладку Задачи.

. В списке задач выберите задачу и откройте окно Свойства: <Название задачи> двойным щелчком мыши по задаче или выбрав в контекстном меню пункт Свойства.

Вне зависимости от выбранного режима запуска задачи вы можете запускать и останавливать задачи в любой момент.
Чтобы запустить или остановить задачу, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства.

. В рабочей области выберите закладку Задачи.

. В списке задач выберите задачу, которую вы хотите запустить или остановить.

. Нажмите на кнопку Запустить или на кнопку Остановить. Кнопки расположены справа от списка задач.

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

- В окне Результаты выполнения задачи. Окно открывается по ссылке Просмотреть результаты, расположенной справа от списка задач, который отображается на закладке Задачи в рабочей области папки Управляемые устройства.

- В списке событий, который отображается на закладке События в рабочей области узла Сервер администрирования.

Вы также можете выполнять следующие действия с задачами:

- копировать задачи из одной папки или группы администрирования в другую;
- экспортировать задачи в файл и импортировать задачи из файла; конвертировать
- задачи предыдущей версии программы; удалять задачи.
- Подробнее об управлении задачами см. в документации Kaspersky Security Center.

Развертывание защиты виртуальной инфраструктуры организациикиента

Развертывание защиты виртуальной инфраструктуры организации-клиента состоит из следующих этапов:

. Установка и настройка всех компонентов программы Kaspersky Security в виртуальной инфраструктуре организации-провайдера антивирусной защиты. Все действия на этом этапе выполняет администратор провайдера.

. Установка Консоли администрирования Kaspersky Security Center на рабочем месте администратора организации-клиента. С помощью Консоли администрирования Kaspersky Security Center вы можете управлять параметрами файловой защиты и параметрами проверки ваших виртуальных машин, а также получать информацию о событиях, которые происходят во время защиты вашей виртуальной инфраструктуры. Подробнее об установке Консоли администрирования см. в документации Kaspersky Security Center.

. Установка плагина управления Kaspersky Security для клиентов на рабочем месте администратора организациикиента.

. Подключение к виртуальному Серверу администрирования Kaspersky Security Center. Вам нужно запустить Консоль администрирования Kaspersky Security Center и указать параметры подключения к виртуальному Серверу администрирования, предоставленные провайдером: адрес, имя пользователя и пароль учетной записи.

. Настройка параметров защиты виртуальных машин от файловых угроз с помощью политики.

Вы также можете создать и настроить задачи проверки для периодической проверки файлов виртуальных машин с использованием новых антивирусных баз.

Установка плагина управления Kaspersky Security для клиентов

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

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

Плагин управления Kaspersky Security для клиентов должен быть установлен на том компьютере, где установлена Консоль администрирования Kaspersky Security Center.

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

. На компьютере, где установлена Консоль администрирования Kaspersky Security Center, запустите файл ksv-tcomponents_6.0.0.XXX_mlg.exe, где 6.0.0.XXX – номер версии программы.

Запустится мастер установки плагина управления Kaspersky Security для клиентов.

. Выберите язык локализации мастера и плагина управления Kaspersky Securityдля клиентов и перейдите к следующему шагу мастера.

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

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

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

Перейдите к следующему шагу мастера.

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

. Дождитесь завершения работы мастера.

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

. Нажмите на кнопку Завершить, чтобы закрыть окно мастера.

Создание политики

Чтобы создать политику для клиентов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства.

. В рабочей области выберите закладку Политики и нажмите на кнопку Новая политика.

Запустится мастер создания политики:

. На первом шаге мастера в списке выберите Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) и перейдите к следующему шагу мастера.

. Введите название новой политики и перейдите к следующему шагу мастера.

. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера.

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

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

сертификат в качестве доверенного, чтобы при следующем подключении к Серверу интеграции не получать сообщение об ошибке сертификата. Для этого установите флажок Установить полученный сертификат и больше не показывать предупреждения для <адрес Сервера интеграции>.

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

. На этом шаге вы можете изменить заданные по умолчанию параметры основного профиля защиты.

Основной профиль защиты назначается по умолчанию всем виртуальным машинам в составе защищаемой инфраструктуры.

Перейдите к следующему шагу мастера.

. Примите решение об участии в Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

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

При необходимости позже вы сможете изменить свое решение.

> Параметры использования KSN (тип и режим использования KSN) определяются политикой провайдера, в области действия которой находятся виртуальные машины клиента.

Перейдите к следующему шагу мастера.

. Завершите работу мастера создания политики.

Созданная политика отобразится в списке политик в папке Управляемые устройства на закладке Политики.

Если вы хотите настроить разные параметры файловой защиты для разных виртуальных машин в составе защищаемой инфраструктуры, вам нужно создать и назначить дополнительные профили защиты в свойствах политики.

Управление защитой от файловых угроз

Параметры, которые Kaspersky Security применяет во время защиты виртуальных машин, задаются с помощью политик.

Kaspersky Security защищает только включенные виртуальные машины, которым назначен профиль защиты.

Когда пользователь или программа обращается к файлу виртуальной машины, Kaspersky Security проверяет этот файл.

- Если в файле не обнаружены вирусы или другие вредоносные программы, Kaspersky Security разрешает доступ к этому файлу.

- Если в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус Зараженный. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или другим вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус Зараженный.

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

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

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

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

- Если установлен уровень безопасности Низкий, применяется поверхностный уровень эвристического анализа. Эвристический анализатор выполняет не все инструкции исполняемых файлов во время проверки исполняемых файлов на наличие вредоносного кода. При таком уровне эвристического анализа вероятность обнаружить угрозу снижена по сравнению со средним уровнем эвристического анализа. Проверка требует меньше ресурсов SVM и проходит быстрее.

- Если установлен уровень безопасности Рекомендуемый, Высокий или Пользовательский, применяется средний уровень эвристического анализа. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет то количество инструкций в исполняемых файлах, которое рекомендовано специалистами "Лаборатории Касперского".

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

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

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

Настройка параметров основного профиля защиты

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

Чтобы настроить параметры основного профиля защиты, выполните следующие действия:

. В блоке Уровень безопасности выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины:

- Если вы хотите установить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его с помощью ползунка.
- Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.
- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку Настройка. В открывшемся окне Параметры уровня безопасности выполните следующие действия:

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

- Не распаковывать составные файлы большого размера
- Максимальный размер проверяемого составного файла N МБ

b. В блоке Производительность укажите значения следующих параметров:

- Ограничивать время проверки файлов
- Проверять файлы не дольше N секунд(ы)

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

- Проверять архивы
- Удалять архивы, если лечение не удалось
- Проверять самораспаковывающиеся архивы
- Проверять вложенные OLE-объекты

- Вредоносные утилиты
- Программы автодозвона
- Рекламные программы
- Другие
- Многократно упакованные файлы

> 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.

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

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

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

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

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

В открывшемся окне Исключения из защиты укажите следующие параметры:

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

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

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

Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме . * | \ : " < > ? /. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: "doc x".

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

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

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

Вы можете исключать из защиты объекты следующих типов:

- Папки. Из защиты исключаются файлы папок, расположенных по указанному пути. Для каждой папки можно указать, следует ли применять исключение из защиты к вложенным папкам.

- Файлы по маске. Из защиты исключаются файлы с указанным именем, файлы, расположенные по указанному пути, или файлы, соответствующие указанной маске.

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

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

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

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

. Нажмите на кнопку ОК в окне Исключения из защиты.

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания политики) или на кнопку Применить (в свойствах политики).

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

Управление дополнительными профилями защиты

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

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

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

. В рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от файловых угроз выберите подраздел Дополнительные профили защиты.

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

В списке дополнительных профилей защиты вы можете выполнять следующие действия:

- Создавать дополнительные профили защиты.
- Изменять имя дополнительного профиля защиты по кнопке Переименовать.
- Изменять параметры дополнительных профилей защиты по кнопке Изменить. Изменение параметров выполняется в окне Параметры защиты. Параметры дополнительного профиля защиты аналогичны параметрам основного профиля защиты.
- Экспортировать параметры дополнительного профиля защиты в файл по кнопке Экспорт. Для сохранения параметров дополнительного профиля защиты нужно указать путь к файлу в формате JSON. Ранее сохраненные параметры вы можете использовать при создании нового дополнительного профиля защиты.
- Удалять дополнительные профили защиты по кнопке Удалить. Если этот профиль защиты использовался для защиты виртуальных машин, программа будет защищать эти виртуальные машины с параметрами профиля защиты, который назначен их родительскому объекту в виртуальной инфраструктуре. Если родительский объект исключен из защиты, программа не будет защищать эти виртуальные машины.

Создание дополнительного профиля защиты

Чтобы создать дополнительный профиль защиты, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте список дополнительных профилей защиты в свойствах политики, для которой вы хотите создать дополнительный профиль защиты.

. Нажмите на кнопку Добавить.

Откроется окно Профиль защиты.

. В открывшемся окне введите имя нового профиля защиты.

Имя профиля защиты не может содержать более 255 символов.

. Если при создании нового профиля защиты вы хотите использовать ранее сохраненные параметры профиля защиты, установите флажок Импортировать параметры из файла и укажите путь к файлу в формате JSON.

. Нажмите на кнопку ОК в окне Профиль защиты.

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

Параметры дополнительного профиля защиты, кроме списка исключений по умолчанию, аналогичны параметрам основного профиля защиты.

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.

. После настройки всех параметров профиля защиты нажмите на кнопку ОК в окне Параметры защиты.
В окне Свойства: <Название политики> в списке дополнительных профилей защиты отобразится новый профиль защиты.

Созданный профиль защиты вы можете назначить виртуальным машинам.

Просмотр защищаемой инфраструктуры в политике

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

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

. В Консоли администрирования Kaspersky Security Center откройте свойства политики:

a. В дереве консоли выберите папку Управляемые устройства.

b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики в разделе Защита от файловых угроз выберите подраздел Защищаемая инфраструктура.

Плагин управления Kaspersky Security пытается автоматически подключиться к Серверу интеграции. Если установить подключение не удалось, откроется окно Подключение к Серверу интеграции. Укажите адрес Сервера интеграции и нажмите на кнопку ОК в окне Подключение к Серверу интеграции.

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

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

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

Информация о защищаемой инфраструктуре

Защищаемая инфраструктура отображается в виде дерева элементов. Корневым элементом является условный объект "Организация vCloud Director", который объединяет все виртуальные Datacenter вашей виртуальной инфраструктуры.

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

Информация о назначении профилей защиты объектам виртуальной инфраструктуры

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

Информация отображается следующим образом:

- Название назначенного явно профиля защиты выделяется черным цветом.
- Название унаследованного от родительского объекта профиля защиты выделяется серым цветом. Название формируется следующим образом: "унаследованный: <N>", где <N> – название унаследованного от родительского объекта профиля защиты.
- Если объекту защищаемой инфраструктуры профиль защиты не назначен (объект исключен из защиты), в графе Профиль защиты отображается значение (Не назначен).

По умолчанию основной профиль защиты назначен корневому объекту "Организация vCloud Director" и наследуется всеми объектами виртуальной инфраструктуры.

Назначение профиля защиты виртуальным машинам

Чтобы назначить виртуальным машинам профиль защиты, выполните следующие действия:

. В свойствах политики выберите подраздел Защищаемая инфраструктура.

. Выберите в таблице одну или несколько виртуальных машин.

Если вы хотите назначить одинаковый профиль защиты всем виртуальным машинам, которые являются дочерними объектами одного виртуального Datacenter, выберите в таблице этот Datacenter. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.

. Нажмите на кнопку Выбрать профиль защиты.

Откроется окно Выбор профиля защиты.

. Выберите один из следующих вариантов:

- Наследовать родительский профиль защиты: <имя>. Выберите этот вариант, чтобы назначить виртуальной машине или другому объекту виртуальной инфраструктуры профиль защиты родительского объекта.
- Использовать профиль защиты. Выберите этот вариант и укажите в раскрывающемся списке имя профиля защиты, чтобы назначить этот профиль защиты виртуальной машине или другому объекту виртуальной инфраструктуры. Список содержит основной профиль защиты и все дополнительные профили защиты, которые вы настроили в этой политике.

. Если у выбранного объекта виртуальной инфраструктуры есть дочерние объекты, профиль защиты назначается объекту и всем его дочерним объектам, включая объекты, которым назначен собственный профиль защиты или которые исключены из защиты. Если вы хотите назначить профиль защиты только выбранному объекту виртуальной инфраструктуры и тем его дочерним объектам, которые наследуют профиль защиты и которые не исключены из защиты, снимите флажок Применить ко всем дочерним объектам.

. Нажмите на кнопку ОК.

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

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

Выключение защиты виртуальных машин от файловых угроз

Чтобы выключить защиту виртуальных машин, выполните следующие действия:

. В свойствах политики выберите подраздел Защищаемая инфраструктура.

. Если вы хотите выключить защиту для одной или нескольких виртуальных машин, выполните следующие действия:

a. Выберите в таблице одну или несколько виртуальных машин.

Если вы хотите выключить защиту для всех виртуальных машин, которые являются дочерними объектами одного виртуального Datacenter, выберите в таблице этот Datacenter. Вы можете выбрать в таблице несколько виртуальных машин или других объектов виртуальной инфраструктуры одновременно, удерживая клавишу **CTRL**.

b. Нажмите на кнопку Выбрать профиль защиты.

Откроется окно Выбор профиля защиты.

c. Выберите вариант Не использовать профиль защиты.

d. Если вы выбрали Datacenter, по умолчанию защита будет выключена для всех виртуальных машин в его составе, включая виртуальные машины, которым назначен собственный профиль защиты. Если вы хотите выключить защиту только для тех виртуальных машин, которые наследуют профиль защиты от родительского объекта, снимите флажок Применить ко всем дочерним объектам.

e. Нажмите на кнопку ОК.

Окно Выбор профиля защиты закроется, в таблице в подразделе Защищаемая инфраструктура для виртуальных машин, которые исключены из защиты, в графе Профиль защиты отобразится значение (Не назначен).

. Если вы хотите выключить защиту для всех виртуальных машин в вашей виртуальной инфраструктуре, снимите флажок Использовать защиту от файловых угроз, расположенный в верхней части окна.

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

Проверка виртуальных машин

Kaspersky Security позволяет выполнять антивирусную проверку файлов виртуальных машин на гипервизоре VMware ESXi. Требуется периодически проверять файлы виртуальных машин с использованием новых антивирусных баз, чтобы предотвратить распространение вредоносных объектов.

Параметры, которые Kaspersky Security применяет во время проверки виртуальных машин, задаются с помощью задач проверки. Kaspersky Security использует для проверки следующие задачи:

- Полная проверка. Задача позволяет выполнять антивирусную проверку файлов всех виртуальных машин в вашей виртуальной инфраструктуре.
- Выборочная проверка. Задача позволяет выполнять антивирусную проверку файлов тех виртуальных машин, которые вы указали в параметрах задачи. Вы можете указывать отдельные виртуальные машины или объекты виртуальной инфраструктуры VMware более высокого уровня иерархии.

Вы можете задавать расписание выполнения задач проверки, запускать задачи проверки вручную и просматривать информацию о ходе и результатах выполнения задач.

Если во время проверки файлов виртуальных машин в файле обнаружены вирусы или другие вредоносные программы, Kaspersky Security присваивает файлу статус Зараженный. Если в результате проверки невозможно однозначно определить, заражен файл или нет (возможно, в файле присутствует последовательность кода, свойственная вирусам или вредоносным программам, или модифицированный код известного вируса), Kaspersky Security также присваивает файлу статус Зараженный.

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

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

Во время проверки виртуальных машин всегда используется глубокий уровень эвристического анализа независимо от выбранного уровня безопасности. Эвристический анализатор выполняет максимальное количество инструкций в исполняемых файлах, что позволяет повысить вероятность обнаружения угрозы.

Если на виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из области проверки.

Особенности проверки виртуальных машин:

- При выполнении задач проверки Kaspersky Security может проверять выключенные виртуальные машины с файловыми системами NTFS, FAT32, EXT2, EXT3, EXT4, XFS, BTRFS.
- При выполнении задач проверки Kaspersky Security может проверять шаблоны виртуальных машин.
- При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется настроить задачу проверки для виртуальных машин, на которых открыт сетевой доступ к папкам и файлам, и включить эти папки и файлы в область проверки задачи.

  При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

После завершения задачи проверки рекомендуется просмотреть список файлов, заблокированных в результате выполнения задачи, и вручную выполнить действия с этими файлами. Например, сохранить копии файлов в недоступном для пользователя виртуальной машины месте и удалить файлы. Предварительно требуется исключить заблокированные файлы из защиты в параметрах профиля защиты, назначенного виртуальным машинам, или временно выключить защиту виртуальных машин, на которых были заблокированы эти файлы. Информацию о заблокированных файлах вы можете просмотреть в выборке событий по событию Файл заблокирован (см. в документации Kaspersky Security Center).

Создание задачи полной проверки

Чтобы создать задачу полной проверки, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства.

. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) → Полная проверка.

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры проверки виртуальных машин.

Перейдите к следующему шагу мастера создания задачи.

. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи.

Перейдите к следующему шагу мастера создания задачи.

. Чтобы настроить расписание запуска задачи, определите значения следующих параметров:

- Запуск по расписанию. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- Запускать пропущенные задачи. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов Вручную и Один раз задача запускается сразу после появления SVM в сети.

  Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов Вручную и Один раз – только на видимых в сети SVM.

- 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.

- Использовать случайную задержку запуска задачи в интервале (мин). Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок Использовать автоматическое определение случайного интервала между запусками задачи.

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

Перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера 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.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную.

Создание задачи выборочной проверки

Чтобы создать задачу выборочной проверки для виртуальных машин клиентов, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center выберите папку Управляемые устройства виртуального Сервера администрирования, соответствующего клиенту.

. В рабочей области выберите закладку Задачи и нажмите на кнопку Новая задача, чтобы запустить мастер создания задачи.

. На первом шаге мастера выберите Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) → Выборочная проверка.

Перейдите к следующему шагу мастера создания задачи.

. Укажите адрес Сервера интеграции и перейдите к следующему шагу мастера создания задачи.

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

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

. Выберите область действия задачи: установите флажки для тех виртуальных машин, которые вы хотите проверить во время выполнения создаваемой задачи. Вы можете указывать отдельные виртуальные машины или их объединения.

Если в виртуальной инфраструктуре присутствуют две или более виртуальные машины с одинаковым идентификатором (vmID), в дереве объектов отображается только одна виртуальная машина. Если эта виртуальная машина выбрана для проверки с помощью задачи выборочной проверки, задача будет выполнена для всех виртуальных машин, которые имеют одинаковый идентификатор (vmID).

Перейдите к следующему шагу мастера создания задачи.

. Настройте параметры проверки виртуальных машин.

Перейдите к следующему шагу мастера создания задачи.

. Если требуется, сформируйте область проверки задачи: укажите местоположения и расширения файлов виртуальных машин, которые нужно проверять или исключить из проверки во время выполнения задачи.

Перейдите к следующему шагу мастера создания задачи.

. Чтобы настроить расписание запуска задачи, определите значения следующих параметров:

- Запуск по расписанию. В раскрывающемся списке выберите режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- Запускать пропущенные задачи. Если требуется, чтобы при очередном запуске программы на SVM предпринималась попытка запуска задачи, установите этот флажок. Для режимов Вручную и Один раз задача запускается сразу после появления SVM в сети.

  Если флажок снят, запуск задачи на SVM производится только по расписанию, а для режимов Вручную и Один раз – только на видимых в сети SVM.

- 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.

- Использовать случайную задержку запуска задачи в интервале (мин). Если вы хотите, чтобы задача запускалась в произвольное время в рамках указанного периода с момента предполагаемого запуска задачи, установите этот флажок, а в поле ввода укажите максимальное время задержки запуска задачи. В этом случае задача запустится в случайное время в рамках указанного периода с предполагаемого момента запуска. Флажок доступен для изменения, если не установлен флажок Использовать автоматическое определение случайного интервала между запусками задачи.

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

Перейдите к следующему шагу мастера создания задачи.

. В поле Имя введите название задачи и перейдите к следующему шагу мастера 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.

Созданная задача отобразится в списке задач. Если в окне Настройка расписания запуска задачи вы задали расписание запуска, задача запустится в соответствии с этим расписанием. Также вы можете в любой момент запустить задачу вручную.

Настройка параметров проверки виртуальных машин в задаче проверки

Вы можете настроить параметры проверки виртуальных машин во время создания задачи (шаг Настройка параметров проверки) или в свойствах задачи после ее создания (раздел Параметры проверки).

Чтобы настроить параметры проверки виртуальных машин, выполните следующие действия:

. Выберите уровень безопасности, в соответствии с которым Kaspersky Security проверяет виртуальные машины. Для этого в блоке Уровень безопасности выполните одно из следующих действий:

- Если вы хотите установить один из предустановленных уровней безопасности (Высокий, Рекомендуемый, Низкий), выберите его с помощью ползунка.
- Если вы хотите изменить уровень безопасности на Рекомендуемый, нажмите на кнопку По умолчанию.
- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку Настройка. В открывшемся окне Параметры уровня безопасности выполните следующие действия:

a. В блоке Проверка архивов и составных файлов укажите значения следующих параметров:
   - Проверять архивы
   - Удалять архивы, если лечение не удалось
   - Проверять самораспаковывающиеся архивы
   - Проверять вложенные OLE-объекты
   - Не распаковывать составные файлы большого размера
   - Максимальный размер проверяемого составного файла N МБ

b. В блоке Производительность укажите значения следующих параметров:
   - Ограничивать время проверки файлов
   - Проверять файлы не дольше N секунд(ы)

c. В блоке Объекты для обнаружения нажмите на кнопку Настройка и укажите в открывшемся окне Объекты для обнаружения значения следующих параметров:
   - Вредоносные утилиты
   - Программы автодозвона
   - Рекламные программы
   - Другие
   - Многократно упакованные файлы

> 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.

. В блоке Проверка включенных виртуальных машин настройте параметры проверки виртуальных машин, которые включены во время выполнения задачи:

- Действие при обнаружении угрозы
- Проверять оптические диски

. В блоке Проверка выключенных виртуальных машин и шаблонов виртуальных машин настройте параметры проверки виртуальных машин, которые выключены или приостановлены во время выполнения задачи, а также шаблонов виртуальных машин:

- Проверять выключенные виртуальные машины
- Проверять шаблоны виртуальных машин
- Действие при обнаружении угрозы

. В блоке Останавливать проверку выберите один из следующих вариантов:

- По истечении N минут(ы) с момента запуска задачи
- После окончания проверки файлов на всех защищенных виртуальных машинах

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Настройка области проверки в задаче проверки

Под областью проверки подразумевается местоположение и расширения файлов виртуальных машин, которые Kaspersky Security проверяет во время выполнения задачи проверки.

Если область проверки не настроена, Kaspersky Security проверяет все файлы виртуальных машин.

При проверке виртуальных машин с операционными системами Windows программа Kaspersky Security не проверяет файлы в сетевых папках. Kaspersky Security может проверять файлы в сетевых папках только при обращении пользователя или какой-либо программы к этим файлам. Если вы хотите регулярно проверять файлы в сетевых папках, вам требуется создать задачу проверки виртуальных машин, папки и файлы которых открыты для сетевого доступа, и включить эти папки и файлы в область проверки задачи.

При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security проверяет файлы в сетевых файловых системах CIFS, если директории, в которые смонтированы сетевые файловые системы CIFS, входят в область проверки задачи. Проверка файлов в сетевых файловых системах NFS не поддерживается.

Вы можете сформировать область проверки задачи во время создания задачи (шаг Выбор области проверки) или в свойствах задачи после ее создания (раздел Область проверки).

Чтобы настроить область проверки задачи, выполните следующие действия:

. 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, вы можете сформировать список объектов, которые требуется исключить из области проверки, с помощью кнопок Добавить, Изменить и Удалить.

Вы можете исключать из области проверки объекты следующих типов:

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

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

  Kaspersky Security не учитывает регистр символов в путях к файлам и папкам, именах и масках файлов, которые требуется исключить из области проверки.

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

В комплект поставки программы входит файл microsoft_file_exclusions.xml, который содержит список исключений, рекомендуемых корпорацией Microsoft (список рекомендуемых исключений Microsoft см. на сайте корпорации Microsoft). Файл microsoft_file_exclusions.xml расположен в папке установки плагина управления Kaspersky Security на компьютере, где установлена Консоль администрирования Kaspersky Security Center. Вы можете импортировать этот файл в исключения задачи проверки. После выполнения импорта Kaspersky Security не проверяет объекты, рекомендуемые корпорацией Microsoft, во время выполнения задачи проверки. Вы можете просмотреть и изменить список этих объектов в таблице Папки и файлы.

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

. Если вы выбрали вариант Проверять все папки и файлы, кроме указанных, в блоке Расширения файлов вы можете указать расширения файлов, которые нужно включить в область проверки или исключить из области проверки.

Для этого выберите один из следующих вариантов:

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

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

  Вы можете задавать расширения файлов в поле через пробел или с новой строки. Расширения файлов могут содержать любые символы, кроме `. * | \ : " < > ? /`. Если в расширении используется символ пробел, то это расширение требуется указывать в кавычках, например: `"doc x"`.

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

Исключенные из проверки папки имеют более высокий приоритет, чем расширения файлов, включенные в область проверки. Если файл находится в папке, исключенной из проверки, то программа не проверяет его, несмотря на то, что расширение файла включено в область проверки.

. Если вы выбрали вариант Проверять только указанные папки и файлы, с помощью кнопок Добавить, Изменить и Удалить сформируйте список папок и файлов на виртуальной машине, которые нужно проверять во время выполнения задачи проверки.

При проверке виртуальных машин с операционными системами Linux программа Kaspersky Security учитывает регистр символов в путях к файлам и директориям, включаемым в область проверки. При проверке виртуальных машин с операционными системами Windows регистр символов в путях к файлам и папкам не учитывается.

Если в списке объектов, которые нужно проверять, вы используете переменную окружения, которая имеет несколько значений в зависимости от разрядности использующего ее приложения, в 64-разрядных операционных системах Windows в область проверки включаются объекты, соответствующие всем значениям переменной. Например, если вы используете переменную %ProgramFiles%, в область проверки включаются объекты, расположенные в папке C:\Program files и в папке C:\Program files (x86).

. Сохраните внесенные изменения, нажав на кнопку Далее (в мастере создания задачи) или на кнопку Применить (в свойствах задачи).

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальных машин, Kaspersky Security может использовать данные, полученные от пользователей программ "Лаборатории Касперского" во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

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

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

В зависимости от расположения инфраструктуры KSN различают:

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

Режим KSN (стандартный KSN или расширенный KSN) влияет на объем данных, которые автоматически передаются в "Лабораторию Касперского" при использовании KSN. Kaspersky Security автоматически отправляет в "Лабораторию Касперского" информацию об использовании KSN, а также может отправлять другую информацию в зависимости от режима использования KSN. Если KSN используется в расширенном режиме, вы соглашаетесь передавать в "Лабораторию Касперского" в автоматическом режиме все данные, перечисленные в Положении о Kaspersky Security Network. В том числе в "Лабораторию Касперского" для проверки 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.

Текст Положения о Kaspersky Security Network вы можете посмотреть в свойствах политики в разделе Параметры KSN.

Информацию о хранении, защите и уничтожении статистической информации, полученной во время использования KSN и переданной в "Лабораторию Касперского", вы можете получить, ознакомившись с Политикой конфиденциальности на веб-сайте "Лаборатории Касперского".

Информацию о том, какой тип и режим KSN использует программа Kaspersky Security, вы может получить у провайдера антивирусной защиты. Параметры использования KSN определяются политикой провайдера.

Участие в Kaspersky Security Network является добровольным. Решение об участии в Kaspersky Security Network принимается при создании политики, его можно изменить в любой момент.

KSN используется в работе Kaspersky Security, только если вы приняли условия Положения о Kaspersky Security Network и провайдер антивирусной защиты включил использование KSN.

Просмотр Положения о Kaspersky Security Network

Чтобы ознакомиться с Положением о Kaspersky Security Network, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры защиты вашей виртуальной инфраструктуры:

a. В дереве консоли выберите папку Управляемые устройства.

b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Параметры KSN.

. Откройте по ссылке Положение о Kaspersky Security Network.
Текст Положения о Kaspersky Security Network откроется в отдельном окне.

Включение и выключение использования Kaspersky Security Network

Включение и выключение использования KSN в работе программы Kaspersky Security выполняется в политике. Если в активной политике использование KSN включено и провайдер антивирусной защиты включил использование KSN, 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 или использование KSN выключено в политике провайдера, службы KSN не используются в работе программы Kaspersky Security.

Чтобы включить или выключить использование KSN в работе программы Kaspersky Security, выполните следующие действия:

. В Консоли администрирования Kaspersky Security Center откройте свойства политики, которая определяет параметры защиты вашей виртуальной инфраструктуры:

a. В дереве консоли выберите папку Управляемые устройства.

b. В рабочей области выберите закладку Политики.

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

. В окне свойств политики выберите раздел Параметры KSN.

. Если вы хотите включить использование KSN в работе программы, выполните следующие действия: a.

Установите флажок Использовать KSN.

b. В открывшемся окне ознакомьтесь с Положением о Kaspersky Security Network.

c. Если вы согласны со всеми пунктами Положения, выберите вариант Я прочитал, понимаю и принимаю условия настоящего Положения о Kaspersky Security Network и нажмите на кнопку ОК.

. Если вы хотите выключить использование KSN, снимите флажок Использовать KSN.

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

Получение информации о состоянии защиты

Компоненты программы Kaspersky Security, установленные на SVM, отправляют на Сервер администрирования Kaspersky Security Center служебные сообщения с информацией о работе программы – события. Информация о событиях сохраняется в базе данных Сервера администрирования.

Выделяют следующие уровни важности событий:

- Критическое событие. Событие критической важности, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке. Может указывать на проблемы в работе Kaspersky Security или на уязвимости в защите виртуальных машин.
- Отказ функционирования. Событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- Предупреждение. Событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky Security и может указывать на возможную проблему в будущем.
- Информационное сообщение. Событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

Вы можете просматривать информацию из базы данных Сервера администрирования в рабочей области узла Сервер администрирования на закладке События.

Информация на закладке События представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства – Критический" содержит только записи об изменении статусов устройств на "Критический". На закладке События содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл. Подробнее о работе с выборками событий см. в документации Kaspersky Security Center.

Уведомление – это сообщение с информацией о событии. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе программы. Для выбора способа уведомления о событиях и настройки других параметров уведомлений о событиях вам нужно обратиться к провайдеру антивирусной защиты.

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

Удаление плагина управления Kaspersky Security для клиентов

Вы можете удалить плагин управления Kaspersky Security для клиентов в интерактивном режиме с использованием стандартных средств удаления программ в операционной системе.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки .

Для этого в списке программ, установленных в операционной системе, требуется выбрать для удаления Kaspersky Kaspersky Security для виртуальных и облачных сред (для клиентов) – плагин управления.

Удаление выполняется с помощью мастера.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

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.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону .
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount .

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" .

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки .

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – 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.

Получение информации для Службы технической поддержки

Отчет для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет, включающий следующие сведения:

- параметры конфигурации SVM; версию гипервизора VMware ESXi; версию сервера VMware
- vCenter Server; версию компонента VMware NSX Manager; версию пакета VMware Tools,
- установленного на защищенной виртуальной машине; список используемых технологий
- VMware (View, DRS, DPM, HA, FT); версию Kaspersky Security Center;
- для компьютера, на котором установлена программа Kaspersky Security Center – версию операционной системы и версию Microsoft .NET Framework.
- Сформированный отчет затем требуется отправить в Службу технической поддержки.
- Получение файлов данных

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас прислать файлы трассировки для компонентов программы и / или файлы системной статистики SVM.

Информацию о том, как получить файлы системной статистики SVM, вы можете посмотреть на странице программы в Базе знаний.

Специальные режимы работы компонентов программы

Для диагностики работы программы специалисты Службы технической поддержки могут попросить вас выполнить следующие действия:

- Включить отладочный режим работы Сервера интеграции. Для включения отладочного режима работы используется специальный параметр конфигурационного файла. Для получения более подробной информации о работе Сервера интеграции может потребоваться настроить дополнительные параметры программы в конфигурационном файле.

- Запустить установку компонентов Kaspersky Security (плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции) в тихом режиме со специальными параметрами командной строки.

- Внести изменения в конфигурационные файлы программы и применить эти изменения.

Подробную информацию, необходимую для выполнения перечисленных действий, вы можете получить у специалистов Службы технической поддержки.

Использование утилит из комплекта поставки программы

Для анализа ошибок в работе Kaspersky Security специалисты Службы технической поддержки могут попросить вас использовать следующие утилиты, входящие в комплект поставки программы:

- inventory_view_format_client, inventory_view_tree_client – утилиты, позволяющие получать сведения о виртуальной инфраструктуре VMware, а также о текущем состоянии защиты и об истории состояний защиты; licenser_client – утилита,
- предназначенная для управления ключами и просмотра информации о лицензии;
- check_policy_client – утилита, позволяющая проверить, использует ли Kaspersky Security политику, полученную от Kaspersky Security Center, или работает с параметрами защиты по умолчанию; ksvscan_client – утилита, предназначенная для
- просмотра информации об установленных базах программы;
- product_status_client – утилита, позволяющая проверить, установлены ли базы программы, активирована ли программа и включена ли защита; qb_client – утилита, предназначенная для работы с резервными копиями файлов в
- резервном хранилище; detect_cache_purge_client – утилита, позволяющая очистить кеш статусов обнаруженных
- объектов;
- event_log_client, emergency_event_log_client – утилиты, позволяющие формировать события для передачи в Kaspersky Security Center;

- tracer_configurator_client – утилита, позволяющая настроить параметры записи информации в файлы трассировки SVM; updater_client – утилита, позволяющая выполнить обновление баз программы или откат
- обновления;
- autopatch_client – утилита, позволяющая выполнить установку патчей программы, загруженных вместе с пакетом обновлений баз программы;

- vicreds – утилита, предназначенная для просмотра или изменения параметров подключения SVM к серверу VMware vCenter Server или к Серверу интеграции;

- ksv_policy_editor, ksv_policy_manager_client – утилиты, позволяющие изменить параметры политики, применяемой на SVM;

- klmover – утилита, позволяющая изменить адрес Сервера администрирования Kaspersky Security Center и режим обмена данными в параметрах конфигурации SVM.

Подробнее об использовании утилит см. на странице программы в Базе знаний.

О файлах трассировки

Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Вы можете просмотреть данные, записанные в файлы трассировки. Для консультации по просмотру данных вам нужно обратиться в Службу технической поддержки "Лаборатории Касперского".

Все файлы трассировки содержат следующие общие данные:

- время события; номер потока выполнения; компонент программы, в результате работы
- которого произошло событие; степень важности события (информационное, предупреждение,
- критическое, ошибка);
- описание события выполнения команды, полученной от компонента программы, и результата выполнения этой команды.
- Файлы трассировки не отправляются автоматически в "Лабораторию Касперского". Вы можете использовать эти файлы при обращении в Службу технической поддержки. Информация, записанная в файлы трассировки, может потребоваться для анализа и выяснения причин возникновения ошибок в работе компонентов программы.

Для работы с файлами трассировки специалисты Службы технической поддержки могут попросить вас использовать скрипт logcontrol.sh, который входят в комплект поставки программы (см. подробнее в Базе знаний).

Файлы трассировки хранятся в незашифрованном виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

О файлах трассировки мастера установки компонентов Kaspersky Security

Информация о ходе и результатах установки, обновления и удаления плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции записывается в файлы трассировки мастера установки компонентов Kaspersky Security. Если установка, обновление и удаление завершилось с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Файлы трассировки мастера установки компонентов Kaspersky Security представляют собой файлы в формате TXT. Они автоматически сохраняются на том компьютере, на котором выполнялась установка, обновление или удаление плагина управления Kaspersky Security, Сервера интеграции и Консоли Сервера интеграции.

В случае установки компонентов Kaspersky Security файлы трассировки сохраняются в архиве

%temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_BundleInitialInstall_logs_<дата и время>.zip, где <дата и время> – дата и время завершения установки.

В случае обновления компонентов Kaspersky Security файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_BundleMajorUpgrade_logs_<дата и время>.zip, где <дата и время> – дата и время завершения обновления.

В случае удаления компонентов Kaspersky Security файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_BundleUninstall_logs_<дата и время>.zip, где <дата и время> – дата и время завершения удаления.

Файлы трассировки мастера установки компонентов Kaspersky Security содержат следующую информацию:

- диагностическую информацию о процессе установки, обновления или удаления компонентов Kaspersky Security;
- имя компьютера, на котором запущена процедура установки, обновления или удаления компонентов Kaspersky Security, и имя пользователя, запустившего процедуру;
- информацию об ошибках, возникающих в процессе установки, обновления или удаления компонентов Kaspersky Security.

О файлах трассировки мастера установки плагина управления Kaspersky Security для клиентов

Информация о ходе и результатах установки, обновления и удаления плагина управления Kaspersky Security для клиентов записывается в файлы трассировки мастера. Если установка, обновление и удаление завершилось с ошибкой, вы можете использовать эти файлы при обращении в Службу технической поддержки.

Файлы трассировки мастера установки плагина управления Kaspersky Security для клиентов представляют собой файлы в формате TXT. Они автоматически сохраняются на том компьютере, на котором выполнялась установка, обновление или удаление плагина управления.

В случае установки плагина управления Kaspersky Security для клиентов файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_(for_tenants)_BundleInitialInstall_logs_<дата и время>.zip, где <дата и время> – дата и время завершения установки.

В случае обновления плагина управления Kaspersky Security для клиентов файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_(for_tenants)_BundleMajorUpgrade_logs_<дата и время>.zip, где <дата и время> – дата и время завершения обновления.

В случае удаления плагина управления Kaspersky Security для клиентов файлы трассировки сохраняются в архиве %temp%\Kaspersky_Security_for_Virtualization_6.0_Agentless_(for_tenants)_BundleUninstall_logs_<дата и время>.zip, где <дата и время> – дата и время завершения удаления.

Файлы трассировки мастера установки плагина управления Kaspersky Security для клиентов содержат следующую информацию:

- диагностическую информацию о процессе установки, обновления или удаления плагина управления Kaspersky Security для клиентов;

- имя компьютера, на котором запущена процедура установки, обновления или удаления плагина управления Kaspersky Security для клиентов, и имя пользователя, запустившего процедуру;

- информацию об ошибках, возникающих в процессе установки, обновления или удаления плагина управления Kaspersky Security для клиентов.

О файлах трассировки SVM

Информация о работе программы может записываться в следующие файлы трассировки, расположенные на SVM:

- на SVM с компонентом Защита от файловых угроз:
  - /var/log/kaspersky/ksv/connector.ksv.log;
  - var/log/kaspersky/ksv/connector.ksvt.log; /var/log/kaspersky/ksv/wdserver.log;
  - var/log/kaspersky/ksv/klmount.log;
  - /var/log/kaspersky/ksv/ksvmain.log;
- на SVM с компонентом Защита от сетевых угроз:
  - /var/log/kaspersky/ksvns/connector.ksv.log;
  - /var/log/kaspersky/ksvns/wdserver.log;
  - /var/log/kaspersky/ksvns/ksvnsmain.log;
- на SVM с компонентом Защита от файловых угроз и на SVM с компонентом Защита от сетевых угроз:
  - /var/log/kaspersky/klnagen64/$klnagent-1103-wd.log;
  - /var/log/kaspersky/klnagen64/$klnagent-1103.log;
  - /var/log/ksv;
  - /var/log/secure;
  - /var/log/messages;
  - /var/log/mr_product_stat_ksv.log; /var/log/mr_system_stat_ksv.log.
- По умолчанию информация о работе программы не сохраняется. Для включения записи информации в файлы трассировки SVM требуется выполнить действия, описанные на странице программы в Базе знаний.

Файлы трассировки SVM, помимо общих данных, могут содержать следующие сведения:

- Имена проверяемых файлов и пути к ним на виртуальной машине. В том числе могут сохраняться персональные данные (фамилия, имя и отчество, адрес электронной почты, имя учетной записи), если эти данные содержатся в путях или именах проверяемых файлов.
- Проверяемые веб-адреса, IP-адреса и имена виртуальных машин, информацию о виртуальной локальной сети (VLAN), информацию о заголовках Ethernet, IP, TCP, UDP для каждого сетевого пакета.
- Сведения о монтировании дисков для проверки выключенных виртуальных машин, списки файловых систем и их идентификаторы.
- Информацию о событиях операционной системы.
- Информацию о событиях, возникающих при взаимодействии с Kaspersky Security Center.
  Информацию о событиях, возникающих во время работы службы watchdog.

-
- Информацию о работе SVM в режиме multitenancy, а также о параметрах конфигурации SVM, получаемых от Сервера интеграции.

О файлах трассировки Сервера интеграции и Консоли Сервера интеграции

Информация о работе Сервера интеграции и Консоли Сервера интеграции может записываться в следующие файлы трассировки:

- %ProgramData%\Kaspersky Lab\VIIS\logs\service.log – файл трассировки Сервера интеграции;
- %ProgramData%\Kaspersky Lab\VIIS Console\logs\console.log – файл трассировки Консоли Сервера интеграции.

Файлы трассировки создаются только после включения записи информации о работе Сервера интеграции и Консоли Сервера интеграции. По умолчанию информация о работе Сервера интеграции и Консоли Сервера интеграции не сохраняется.

Вы можете включить запись информации в файлы трассировки Сервера интеграции и Консоли Сервера интеграции, а также изменить уровень детализации информации в файлах трассировки с помощью конфигурационных файлов:

- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIIS\NIog.config – для файла трассировки Сервера интеграции;
- %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIIS Console\NLog.config – для файла трассировки Консоли Сервера интеграции.

За подробной информацией вы можете обратиться к специалистам Службы технической поддержки.

Если вы включили запись информации в файл трассировки Сервера интеграции, вы можете открыть для просмотра этот файл по ссылке Посмотреть файл трассировки в разделе Параметры Сервера интеграции Консоли Сервера интеграции. Ссылка доступна, только если Консоль Сервера интеграции установлена на том же компьютере, что и Сервер интеграции.

В файле трассировки Сервера интеграции может сохраняться следующая информация:

- Диагностическая информация о работе Сервера интеграции, его загруженности, о результатах проверки целостности данных.
- Заголовки и содержимое http-запросов, которые отправляет и принимает Сервер интеграции в процессе своей работы.
- IP-адреса SVM и компьютера, на котором установлена Консоль администрирования Kaspersky Security Center и плагин управления Kaspersky Security, если Консоль администрирования Kaspersky Security Center установлена отдельно от Сервера администрирования Kaspersky Security Center.
- Трассировка запросов к Серверу интеграции.
- Описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами.
- Имена внутренних учетных записей Сервера интеграции.

  IP-адреса или полные доменные имена (FQDN) серверов VMware vCenter Server, к которым подключается Сервер интеграции.
- Информация о процессе регистрации служб Kaspersky Security.
- Информация о процессе изменения параметров Kaspersky Security.

В файле трассировки Консоли Сервера интеграции может сохраняться следующая информация:

- Диагностическая информация о работе Консоли Сервера интеграции.
- Трассировка параметров командной строки и результаты их проверки.
- Заголовки и содержимое http-запросов, которые отправляет и принимает Консоль Сервера интеграции в процессе своей работы.
- Информация о переходах по разделам Консоли Сервера интеграции и работе с элементами интерфейса.
- IP-адрес Сервера администрирования Kaspersky Security Center.
- Номера портов для взаимодействия с Сервером администрирования Kaspersky Security Center через Агент администрирования Kaspersky Security Center.
- Описание исключений и ошибок, возникающих при работе с внутренними подсистемами и внешними службами.
- Имена внутренних учетных записей Сервера интеграции.
- IP-адреса или полные доменные имена (FQDN) серверов VMware vCenter Server, VMware vCloud Director и VMware NSX Manager, к которым подключается Сервер интеграции.

Источники информации о программе

Страница Kaspersky Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security 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 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 Kaspersky Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

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

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

Приложение. Краткая инструкция по установке программы

Перед началом установки программы убедитесь, что:

. Выполняются все программные и аппаратные требования Kaspersky Security.

. Виртуальная инфраструктура VMware подготовлена к установке Kaspersky Security:

a. Гипервизоры VMware ESXi объединены в один или несколько кластеров VMware.

b. На каждом гипервизоре выбраны сеть и хранилище для служебных виртуальных машин и SVM (параметры Agent VM Settings, см. подробнее в документации к продуктам VMware).

c. На каждом кластере VMware, на котором будут развернуты SVM с компонентом Защита от файловых угроз, развернута служба Guest Introspection.

d. На каждом кластере VMware, на котором будут развернуты SVM с компонентом Защита от сетевых угроз, установлены компоненты VMware NSX. См. подробнее в Базе знаний .

e. На каждой виртуальной машине, которую вы хотите защищать с помощью Kaspersky Security, установлен Guest Introspection Thin Agent. См. подробнее в документации к продуктам VMware .

f. Для VMware NSX for vSphere используется лицензия NSX for vSphere Advanced или NSX for vSphere Enterprise (если вы планируете установить компонент Защита от сетевых угроз).

. Все файлы образов SVM загружены с веб-сайта "Лаборатории Касперского" и размещены в одной папке на сетевом ресурсе, доступном по протоколу HTTP или HTTPS. Например, образы SVM опубликованы на Вебсервере Kaspersky Security Center.

. Открыты порты, которые требуются для работы программы, и созданы учетные записи, которые требуются для установки и работы программы.

Перед началом установки программы Kaspersky Security рекомендуется закрыть Консоль администрирования Kaspersky Security Center.

Чтобы установить программу, выполните следующие действия:

. Установите основной плагин управления Kaspersky Security и Сервер интеграции.

. Если вы хотите использовать программу в режиме multitenancy, установите плагин управления Kaspersky Security для клиентов.

При первом запуске Консоли администрирования Kaspersky Security Center после установки плагинов управления Kaspersky Security автоматически запускается мастер первоначальной настройки управляемой программы. Мастер позволяет создать

политики по умолчанию и задачи. Если мастер первоначальной настройки управляемой программы не запустился автоматически, рекомендуется запустить его вручную.

. Запустите Консоль Сервера интеграции и настройте параметры подключения Сервера интеграции к одному или нескольким серверам управления виртуальной инфраструктурой.

. В консоли Сервера интеграции с помощью мастера выполните регистрацию служб Kaspersky Security в VMware NSX Manager.

. В консоли VMware vSphere Web Client разверните SVM с компонентом Защита от файловых угроз и SVM с компонентом Защита от сетевых угроз на гипервизорах VMware ESXi.

. В консоли VMware vSphere Web Client настройте группы безопасности NSX (NSX Security Group) и политики безопасности NSX (NSX Security Policy) и примените политики безопасности на группы безопасности NSX.

Если вы хотите использовать программу в режиме multitenancy, настройте защиту организаций-клиентов:

. В Консоли администрирования Kaspersky Security Center для каждого клиента, виртуальные машины которого требуется защищать, создайте виртуальный Сервер администрирования и учетную запись, под которой администратор клиента будет подключаться к виртуальному Серверу администрирования.

. В Консоли администрирования Kaspersky Security Center создайте учетную запись, под которой Сервер интеграции будет подключаться к Серверу администрирования Kaspersky Security Center. Подключение требуется для получения информации о виртуальных Серверах администрирования, созданных в Kaspersky Security Center, и для настройки соответствий между виртуальными Серверами администрирования и организациями vCloud Director, которые содержат виртуальные машины клиентов.

. В Консоли Сервера интеграции выполните подключение Сервера интеграции к Серверу администрирования Kaspersky Security Center и настройте список соответствий между организациями vCloud Director и виртуальными Серверами администрирования Kaspersky Security Center.

. Передайте администратору клиента следующую информацию: адрес Сервера интеграции, адрес виртуального Сервера администрирования, настроенного для этого клиента, имя и пароль учетной записи для подключения к виртуальному Серверу администрирования.

После установки программы подготовьте программу к работе и выполните первоначальную настройку:

. Активируйте программу на всех новых SVM и убедитесь, что базы программы обновлены на всех новых SVM.

. Включите защиту виртуальных машин от файловых и сетевых угроз. По умолчанию Kaspersky Security не защищает виртуальные машины.

Глоссарий

Kaspersky CompanyAccount

Портал, предназначенный для отправки электронных запросов в "Лабораторию Касперского" и отслеживания их обработки специалистами "Лаборатории Касперского".

Kaspersky Security Network (KSN)

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

OLE-объект

Объект, который присоединен к другому файлу или встроен в другой файл с использованием технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel, встроенная в документ Microsoft Office Word.

SVM

Secure virtual machine, виртуальная машина защиты. Виртуальная машина на гипервизоре VMware ESXi, на которой установлен компонент программы Kaspersky Security.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и компонентами программы Kaspersky Security, установленными на SVM. Компонент Агент администрирования является единым для всех программ "Лаборатории Касперского" для Windows. Для программ "Лаборатории Касперского" для Novell, UNIX и Mac существуют отдельные версии Агента администрирования.

Активация программы

Процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

Группа администрирования

Набор устройств, объединенных в Kaspersky Security Center в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы администрирования могут входить другие группы. Для каждой из установленных в группе администрирования программ могут быть созданы групповые политики и сформированы групповые задачи.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Задача активации программы

Добавляет лицензионный ключ на SVM, выбранные при создании задачи.

Задача выборочной проверки

Определяет параметры проверки файлов указанных виртуальных машин из области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

Задача обновления баз программы

Во время выполнения задачи Kaspersky Security Center автоматически распространяет и устанавливает обновления баз программы на SVM.

Задача отката обновлений

Во время выполнения задачи Kaspersky Security Center откатывает последнее обновление баз программы на SVM.

Задача полной проверки

Определяет параметры проверки файлов всех виртуальных машин, находящихся в области действия задачи. Область действия задачи зависит от расположения задачи в иерархии групп администрирования Kaspersky Security Center и от плагина управления Kaspersky Security, с помощью которого вы создаете задачу.

Защищаемая инфраструктура кластера KSC

Объекты виртуальной инфраструктуры VMware под управлением сервера VMware vCenter Server или сервера VMware vCloud Director, соответствующего кластеру KSC.

Источник обновлений

Ресурс, содержащий обновления баз и модулей программы для программ "Лаборатории Касперского". Источником обновлений для Kaspersky Security является хранилище Сервера администрирования Kaspersky Security Center.

Кластер KSC

В программе Kaspersky Security Center: набор SVM, развернутых на гипервизорах VMware ESXi под управлением автономного сервера VMware vCenter Server или под управлением всех серверов VMware vCenter Server, подключенных к одному VMware vCloud Director.

Ключ для рабочих станций

Ключ программы для защиты виртуальных машин с операционными системами для рабочих станций.

Ключ для серверов

Ключ программы для защиты виртуальных машин с операционными системами для серверов.

Ключ с ограничением по процессорам

Ключ программы для защиты виртуальных машин независимо от типа установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин, работающих на гипервизорах, в которых используется определенное количество физических процессоров.

Ключ с ограничением по ядрам

Ключ программы для защиты виртуальных машин независимо от типа установленной на них операционной системы. В соответствии с лицензионным ограничением программа используется для защиты всех виртуальных машин на гипервизорах, в которых используется определенное количество ядер физических процессоров.

Код активации

Код, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Security. Этот код требуется для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр в формате XXXXX-XXXXXXXXXX-XXXXX.

Лицензионное соглашение

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Лицензионный ключ (ключ)

Уникальная буквенно-цифровая последовательность. Лицензионный ключ обеспечивает использование программы в соответствии с условиями Лицензионного соглашения (типом лицензии, сроком действия лицензии, лицензионными ограничениями). Вы можете использовать программу только при наличии в ней лицензионного ключа.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Основной профиль защиты

Основной профиль защиты формируется автоматически во время создания политики и содержит параметры защиты от файловых угроз. Удалить основной профиль защиты нельзя, но можно изменить значения его параметров.

Политика

Определяет параметры защиты виртуальных машин от вирусов и других вредоносных программ, параметры защиты виртуальных машин от сетевых угроз, параметры резервных хранилищ и параметры использования Kaspersky Security Network.

Профиль защиты

Профиль защиты определяет в политике параметры защиты виртуальных машин от файловых угроз. Политика может включать несколько профилей защиты (основной профиль защиты и дополнительные профили защиты).

Профили защиты назначаются виртуальным машинам и другим объектам виртуальной инфраструктуры VMware. Одному объекту виртуальной инфраструктуры может быть назначен только один профиль защиты. SVM защищает виртуальную машину с теми параметрами, которые указаны в назначенном ей профиле защиты.

Виртуальные машины, которым не назначен профиль защиты, исключаются из защиты.

Режим multitenancy

Режим работы программы, при котором один экземпляр программы, установленный в инфраструктуре организациипровайдера антивирусной защиты, позволяет нескольким организациям-клиентам независимо управлять защитой своей виртуальной инфраструктуры.

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.

Резервное хранилище

Специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Составной файл

Составной файл представляет собой несколько отдельных файлов, которые хранятся в одном физическом файле, к каждому из этих файлов можно получить доступ. Примерами составных файлов являются архивы, инсталляционные пакеты, вложенные OLE-объекты, файлы почтовых форматов. Распространенная практика сокрытия вирусов – внедрение их в составные файлы. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать.

Файл ключа

Файл вида xxxxxxxx.key, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Security. Файл ключа требуется для активации программы.

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

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

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

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

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

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

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

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

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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

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

Microsoft, Active Directory, 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, VMware NSX Manager, VMware NSX for vSphere, VMware vCenter, VMware vCenter Server, VMware vCloud Director, 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.